NAVAL COMMUNICATIONS SECURITY MATERIAL SYSTEM
1560 Colorado Avenue
Andrews AFB, MD 20762-6108

EKMS-1B

ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS) POLICY AND PROCEDURES FOR NAVY EKMS TIERS 2 & 3

2250
Ser N5/
05 Apr 2010

Article I. LETTER OF PROMULGATION

1. **PURPOSE.** EKMS-1B prescribes the minimum policies for issuing, accounting, handling, safeguarding, and disposing of COMSEC (Communications Security) material. Also included are policies for cryptographic and physical security involving COMSEC material and facilities. This document is not designed to be read from cover-to-cover. It is meant as a ready-reference for supervisors and managers involved in the management, use and accounting of COMSEC material. Readers can find many immediately useful sections: a glossary of EKMS terms, a section on how to stand up an EKMS account, a section on how to conduct a semi-annual account inventory, etc.

2. **BACKGROUND.** The Electronic Key Management System (EKMS) which operates through the use of a Local Management Device/Key Processor (LMD/KP) provides the capability for the automated generation, 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. 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.

3. **APPLICABILITY.**

a. EKMS-1B policies apply to COMSEC materials held by U.S. Navy, U.S. Marine Corps, U.S. Coast Guard, and Military Sealift Command EKMS-numbered accounts. These provisions apply to all who require access to or the use of COMSEC material within EKMS. All such personnel must be aware that non-compliance or deviation from the prescribed procedures can jeopardize the security of the United States and could result in prosecution of the parties concerned under the espionage laws, Title 18. U.S.C., Sections 793, 794, and 798.

b. Commands whose holdings include Two-Person Controlled (TPC) Sealed Authentication System (SAS) keying material are advised of the following: The policies governing the handling, safeguarding, and use of TPC SAS material are not in this manual but can be found in CJCSI 3260.01(series), a required directive for all commands with TPC SAS material holdings. See Article 721 for contact information to obtain a copy of the document, if required. Requests for disposition of SAS/TPC material must be addressed to the Controlling Authority per CJCSI 3260.01(series), info the COR. The COR is not authorized to provide disposition instructions for this material.

4. **SCOPE.** The policies in this manual 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.** EKMS-1B is effective upon receipt and supersedes EKMS-1A (March 2007).

6. **REPRODUCTION.** EKMS 1B is authorized for reproduction, distribution and use in any operational environment and is available via the NCMS SIPRNET Collaboration at-Sea (CAS) website located at: http://www.uar.cas.navy.smil.mil/secret/navy/39/site.nsf. This manual is also available via NIPR on the INFOSEC website located at: https://infosec.navy.mil

7. **COMMENTS.** Submit comments, recommendations, and suggestions for changes to Naval Communications Security Material System (NCMS).

CORREIA.JOAQUIN.S.1174903790

Digitally signed by CORREIA.JOAQUIN.S.1174903790
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=CORREIA.JOAQUIN.S.1174903790
Date: 2015.02.10 09:42:50 -05'00'

J. S. CORREIA

RECORD OF AMENDMENTS

AMEND NUMBER/ IDENTIFICATION	DATE ENTERED (YYMMDD)	ENTERED BY (Signature, Rank/Rate, Command Title)
AMD 1 (ALCOM 108/10)	2010/07/06	M. J. PHILLIPS, IA-04, NCMS
AMD 2 (ALCOM 161/10)	2010/10/29	M. J. PHILLIPS, IA-04, NCMS
AMD 3 (ALCOM 020/11)	2011/01/29	M. J. PHILLIPS, IA-04, NCMS
AMD 4 (ALCOM 085/11)	2011/04/30	M. J. PHILLIPS, IA-04, NCMS
AMD 5 (ALCOM 213/11)	2011/12/29	M. J. PHILLIPS, IA-04, NCMS
AMD 6 (ALCOM 111/12)	2012/06/29	M. J. PHILLIPS, GG-13, NCMS
AMD 7 (ALCOM 079/13)	2013/04/23	M. J. PHILLIPS, GG-13, NCMS
AMD 8 (ALCOM 152/14)	2014/10/17	C. W. BENKO, LT, NCMS
AMD 9 (ALCOM 030/15)	2015/02/06	C. W. BENKO, LT, NCMS

RECORD OF PAGE CHECKS

DATE CHECKED	CHECKED BY (SIGNATURE, RANK/RATE, COMMAND TITLE)	DATE CHECKED	CHECKED BY (SIGNATURE, RANK/RATE, COMMAND TITLE)

"SNAPSHOT" of EKMS 1B
ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS) POLICY & PROCEDURES MANUAL

ANNEXES

TABLE OF CONTENTS

CHAPTER 1 -- COMMUNICATIONS SECURITY (COMSEC) MATERIAL CONTROL SYSTEM (CMCS)

CHAPTER 2 -- INTRODUCTION TO COMSEC MATERIAL

RESPONSIBILITIES

CHAPTER 5 -- SAFEGUARDING COMSEC MATERIAL AND FACILITIES

CHAPTER 6 -- MAINTAINING COMSEC MATERIAL ALLOWANCE

CHAPTER 7 -- CONTROL AND DOCUMENTATION REQUIREMENTS FOR COMSEC MATERIAL

FIGURES:

CHAPTER 9 -- COMSEC INCIDENT REPORTING

CHAPTER 10 -- PRACTICES DANGEROUS TO SECURITY (PDSs)

CHAPTER 11 -- MANAGEMENT OF ELECTRONIC KEY

ANNEXES

CHAPTER 1 - COMMUNICATIONS SECURITY (COMSEC) MATERIAL CONTROL SYSTEM (CMCS)

CHAPTER 1 - COMMUNICATIONS SECURITY (COMSEC) MATERIAL CONTROL SYSTEM (CMCS)

101. INTRODUCTION TO THE COMSEC MATERIAL CONTROL SYSTEM (CMCS):

a. Communications Security (COMSEC) material is used to protect U.S. Government and partner classified or sensitive unclassified communications or information from unauthorized persons.

b. The protection of vital and sensitive information moving over government communications systems is crucial to the effective conduct of the government, and specifically, to the planning and execution of military operations. To this end, a system has been established to distribute, control, and safeguard COMSEC material. This system, which consists of production facilities, COMSEC Central Offices of Records (CORs), distribution facilities (i.e., depots), and EKMS accounts, is known collectively as the CMCS.

c. COMSEC material is managed in EKMS/COMSEC accounts throughout the federal government to include military departments and civil agencies supporting the federal government.

105. INTRODUCTION TO THE ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS):

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 overall EKMS architecture consists of four layers or tiers. Each tier is part of a higher tier. For example, a Tier 3 (Local Element), must be assigned to a Tier 2 (EKMS Account).

a. **TIER 0 (Central Facility)** – EKMS Tier 0 consists of the National Security Agency’s (NSA) Fort Meade and Finksburg Key Facilities. Tier 0 provides centralized key management services for all forms of COMSEC key.

b. **TIER 1** - This layer of the EKMS serves as the intermediate key generation and distribution center, central offices of record (COR), privilege managers, and registration authorities for EKMS/COMSEC accounts. Management of the system is a cooperative effort involving the Navy, NSA, Joint Staff, (J6), Army, and Air Force.

(1) **Common Tier 1 (CT1)** – CT1 is comprised two Primary Tier 1 sites (Lackland AFB, San Antonio, TX and Ft. Huachuca, AZ) and other physical distribution handling systems at several service sites. CT1 houses the physical EKMS servers that are used for accounting and will provide for the generation and distribution of many traditional key types for large nets.

(2) **SERVICING PRIMARY TIER 1 SEGMENT (PT1S) –** A term used to refer to the Tier 1 site having primary COR (Central Office of Record) responsibility for a portion of the Tier 2 accounts.

c. **TIER 2** - The layer of EKMS comprised of the EKMS Accounts that manage key and other COMSEC material. Tier 2 accounts are equipped with a Local Management Device (LMD) that runs Local COMSEC Management Software (LCMS) and interfaces with a Key Processor (KP). This suite of equipment is referred to as a LMD/KP. A small number of Tier 2 accounts whose holdings are restricted to equipment are "LMD-only accounts". Tier 2 accounts receive electronic key from Tier 0, Tier 1 or other Tier 2 accounts.

d. **TIER 3** - Tier 3 is synonymous with Local Elements (LEs). Tier 3 is the lowest tier or layer of the EKMS architecture. Tier 3 may include the AN/CYZ-10 (Data Transfer Device (DTD), AN/PYQ-10 (Simple Key Loader (SKL), other means used to fill key to End Cryptographic Units (ECUs), hard copy material holdings, and STE keying material using Key Management Entities (KMEs). Tier 3 entities never receive electronic key directly from Tier 0 or Tier 1.

110. **NATIONAL SECURITY AGENCY (NSA):** The National Security Agency serves as Tier 0 and is the executive agent for developing and implementing national level policy affecting the control of COMSEC material. NSA is also responsible for the production and distribution of most COMSEC material used to secure communications as well as for the development and production of cryptographic equipment.

115. **ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS) CENTRAL FACILITY (CF):** The EKMS CF operates as part of the NSA and functions primarily as a high volume key generation and distribution center. As such, it provides commands with keys currently produced by NSA that cannot be generated locally or must be generated by Tier 0 for other reasons. The CF will interoperate with commands through a variety of media, communication devices, and networks, allowing for the automated ordering of COMSEC key and other materials generated and distributed by NSA.

120. DEPARTMENT OF THE NAVY (DON): The DON administers its own CMCS, which includes Navy, Marine Corps, Coast Guard, and Military Sealift Command (MSC) EKMS and KMI Accounts. DON system implements national policy, publishes procedures, establishes its own EKMS accounts and serves as a Service Authority (SERVAUTH) for COMSEC material.

a. **CHIEF OF NAVAL OPERATIONS (CNO)**: Overall responsibility and authority for implementation of National COMSEC policy within the DON. The Head, Navy Information Assurance (IA) Branch is the COMSEC resource sponsor and is responsible for consolidating the COMSEC programming, planning and implementation of policy and technical improvements.

> **NOTE: DON CIO as the Executive Agent is overall responsible for DON COMSEC policy and oversight. The Deputy Under Secretary of the Navy for Plans, Policy, Oversight and Integration (DUSN PPOI) is the DON's Security Executive responsible for DON security policy.**

b. **HEADQUARTERS MARINE CORPS (C4 CY)**: HQMC C4 CY serves as COMSEC resource sponsor for the Marine Corps. The department functions as the USMC Service Authority and coordinates with CNO, COMNAVIDFOR, and NCMS to establish, promulgate, and oversee EKMS account management matters unique to the Marine Corps. The C4/CY is the focal point for requirements and administration for all Marine Corps EKMS accounts.

c. **COMMANDER, U.S. COAST GUARD C4IT SERVICE CENTER, INFORMATION ASSURANCE BRANCH (C4ITSC-BOD-IAB)**: Acts as the USCG Service Authority (SA) and exercises overall authority for USCG COMSEC matters and also serves as the USCG Program Manager and Principal Agent for the USCG COMSEC Program and also functions as the USCG; Service Authority, Evaluating ~~Closing Action~~
AMD-9 Authority, Command Authority (CA) and USCG ISIC. This office promulgates USCG COMSEC Program policy and exercises service wide management of Coast Guard EKMS accounts including hardware and software allowances. The branch also acts as principal USCG liaison for COMSEC with CNO, NCMS and the Tier 1s to ensure that all USCG EKMS Accounts have the necessary resources to operate effectively. The Office coordinates with other Military

Services, the Director NSA, other Federal, State, and Local law enforcement entities to ensure secure/privacy communications interoperability.

d. **NAVAL COMMUNICATIONS SECURITY MATERIAL SYSTEM (NCMS)**: Administers the DON COMSEC program and is the Service Authority for DON. NCMS performs these specific functions:

1. Maintain the central office of record, ensuring the proper storage, distribution, inventory, accounting, and overall safeguarding of COMSEC materials for the Navy, Marine Corps, Coast Guard, Military Sealift Command, and joint and allied commands as required.

2. As the DON COMSEC policy author, draft and publish COMSEC policy directives, standards, and procedures pertaining to COMSEC material security, distribution, training, handling, and accounting within the DON to ensure National level policies are followed and enforced.

3. Operate, maintain, and exercise administrative, operational, and technical control over the CMIO for distribution of COMSEC equipment, in order to control, warehouse and distribute keying material for all Navy.

4. Monitor compliance with national standards of the Protective Packaging Program for cryptographic keying material.

5. Coordinate fleet requirements for the acquisition of all COMSEC material and publications for DON commands.

6. Establish and disestablish DON EKMS numbered accounts.

7. Based on Combatant Commanders' requirements, ensure distribution of COMSEC material to Vault Distribution Logistics System (VDLS) components to ensure quantities are sufficient for EKMS account requirements, exercises, and contingency operations.

8. Provide disposition instructions for excess, failed or obsolete COMSEC equipment or keying material for which NCMS is the Controlling Authority or Command Authority, as applicable.

9. As the COMSEC Incident Monitoring Activity (CIMA) for the DON; evaluate instances of loss, compromise, and procedural violations of COMSEC procedures to determine the adequacy of existing procedures as well as overall compliance with existing

policy as the DON COMSEC incident monitoring activity and the DON COMSEC Inspection Program manager.

10. Establish standards for the ~~COMSEC Inspection~~ COR Audit Program.

AMD-9

11. Manage the DON COMSEC Training Program and provide, via ~~CMS Advice and Assistance (A&A) Training~~ COR Audit Teams, worldwide COMSEC advice and assistance to customers.

12. As the DON Registration Authority, register and assign EKMS IDs to Key Management Entities (KME), order initialization keys for KPs and for maintain registration data on its KMEs in the EKMS Directory Service.

13. Act as the FIREFLY Point of Contact for modern key privileges.

14. Resolve COMSEC related technical queries and conflicts with members of DON and the National COMSEC community.

15. Coordinate with Deputy CNO, Information Dominance (CNO N2/N6), Director National Security Agency, and U.S. Fleet Cyber Command regarding COMSEC equipment and associated infrastructure releasability to foreign governments and international organizations.

16. Review requests for and authorize the release of DON COMSEC material to contractors and assist DIRNSA in the establishment of COMSEC accounts as necessary.

17. Serve as the final waiver authority for DON COMSEC policies and physical security requirements.

18. Act as the Requirements Sponsor for EKMS, CT3-DMD, KMI, and CWMS.

19. Act as the FORTEZZA Approving Authority.

20. Act as the Parent COMSEC Account for the Offices of the Chief of Naval Operations, the Secretary of the Navy, and others as directed.

e. **COMSEC MATERIAL ISSUING OFFICE (CMIO)**: Receives, stores, and ships Ready for Issue (RFI) equipment and is the Physical Material Handling Segment (PMHS) for Navy in the EKMS.

f. **UNITED STATES NATIONAL DISTRIBUTION AUTHORITY (USNDA):** The consolidated (Air Force, Army, Navy and NSA) COMSEC distribution facility for keying material. The USNDA processes and automatically ships Reserve on Board (ROB) material to the Defense Courier Station (DCS) based on the information reflected on the units U.S. Transportation Command Form-10.

125. CONTROLLING AUTHORITY (CONAUTH): In the context of the CMCS, each item of traditional COMSEC material is controlled or managed by a designated official known as a CONAUTH. A CONAUTH is responsible for evaluating COMSEC incidents and authorizing the issue/destruction of COMSEC material under their control. By definition, a CONAUTH is the command which has designated responsibility for directing the establishment and operation of a cryptonet/circuit and managing the operational use and control of keying material assigned to a cryptonet/circuit. CONAUTH responsibilities are detailed in Annex C. For modern (asymmetric key), there is no Controlling Authority. The responsibilities are performed by a Command Authority.

126. SERVICE AUTHORITY:

The role of the Service Authority is defined within each Service and may be executed by more than one person or agency within that Service. Service Authority activities within each military service include oversight for COMSEC operations, policy, procedures, and training. Service Authority roles may include:

- Cryptographic hardware management and distribution +control, including Foreign Military Sales (FMS).
- Approving account establishments.
- Approving authority for Certification Approval Authorities (CAAs).
- Implementing COMSEC Material Control System (CMCS)/Key Management Infrastructure (KMI) policy and procedures.
- Direct operational support.
- Final adjudication authority for determining when reported COMSEC incidents result in COMSEC insecurities.
- Ensuring service compliance with COMSEC access program Requirements.
- Standing membership on KMI working groups and the CT1 Joint Configuration Control Board (JCCB).

130. IMMEDIATE SUPERIOR IN COMMAND (ISIC): Responsible for the administrative oversight of all COMSEC matters for their subordinate commands. All COMSEC matters fall under the purview of the Administrative Command (ADCON). NCMS will refer to the following sources to determine ADCON:

-USN: Standard Navy Distribution List (SNDL)
-USMC: EKMS ISIC and Inspectors Alignment for
Marine Corps EKMS Accounts (COMSEC Advisory)
-USCG: Commandant Notice 5440

135. STAFF CMS RESPONSIBILITY OFFICER (SCMSRO): A flag or general officer in command status, or the Deputy Commander or Chief of Staff, may either assume personal responsibility for routine COMSEC matters or may designate the responsibility to a staff officer (O-4/GS-12, Pay Band 2, or above). Officers not meeting the above requirement may not designate a SCMSRO. A SCMSRO may exist at a command with an account or LE.

140. COMMANDING OFFICER (CO): The CO is responsible for properly administering his/her command's EKMS account and ensuring compliance with established policy and procedures.

> **NOTE: Throughout this manual, responsibilities/duties applicable to Commanding Officers apply equally to Staff CMS Responsibility Officers (SCMSRO) and Officers-in-Charge (OIC), unless otherwise indicated.**

145. EKMS ACCOUNT: An EKMS account is an administrative entity in which custody and control of COMSEC material are maintained. Within the EKMS architecture, these accounts are also called Tier 2 accounts. Each EKMS Tier 2 account is assigned and identified by a six-digit EKMS account number, which also serves as the account's EKMS ID.

150. LCMS SYSTEM ADMINISTRATOR (SA): SA functions are normally performed by the EKMS Manager and Primary Alternate. Responsibilities include but are not limited to; SCO-Unix and LCMS account creation/deletion, password resets, and database management including backups and registration of accounts and/or local elements. A minimum of two LCMS System Administrators must be appointed. If it is determined that a third or fourth LCMS System Administrator must be appointed, candidates must be selected from among alternate EKMS Managers (e.g., secondary alternate).

155. EKMS MANAGER: An individual designated in writing by the CO to manage COMSEC material issued to an EKMS account. The EKMS Manager is the CO's primary advisor on matters concerning the security and handling of COMSEC material and the associated records, reports, and audits. The individual must be a U.S.

Military member or Government Civil Service employee.

> **NOTE: Throughout this manual, the use of the term "EKMS Manager" will apply to account managers and their alternates as well as to issuing local elements and their alternates, unless otherwise specified.**

160. ALTERNATE EKMS MANAGER(S): The individual(s) designated in writing by the CO responsible for assisting the EKMS Manager in the performance of his/her duties and assuming the duties of the EKMS Manager in his/her absence. The alternate shares equally with the EKMS Manager the responsibility for the proper management and administration of an EKMS account. The individual must be a U.S. Military member or Government Civil Service employee.

165. LOCAL ELEMENT (LE): There are two variants of Local Elements: LE (Using) and LE (Issuing). Both reside at the Tier 3 layer in the EKMS architecture. The primary difference between LE (Using) and LE (Issuing) is that LE Using (Users) are normally work centers within the same organization in which the account resides and which receive COMSEC material from their activities EKMS account for use in their respective division or work center. Typically, these entities operate on a watch-to-watch basis and not for issuing on a Local Custody basis. Examples include Radio, CIC, SATCOM, Tech Control, etc…

LE (Issuing) receives material from their own parent EKMS account or another established account to issue material on a local custody basis. These entities are generally external entities (squadrons, mobile users, etc…) but may, dependent upon organizational structure and mission, be internally structured.

The issuance of COMSEC material from an established EKMS account to either LE Users or LE Issuing which are not part of the organization owning the EKMS account (external) must be established and supported through a formal Letter of Agreement (see Article 445).

> **NOTE: Throughout this manual, the terms "Letter of Agreement", "Memorandum of Agreement" and "Memorandum of Understanding" will be used interchangeably.**

LE (Issuing) units are required to properly account for, store, issue, inventory, destroy and safeguard COMSEC material provided to them. They are required to create and retain required accounting documentation (e.g., LCI and local destruction records). LE (Issuing) personnel must be appointed in writing and meet the designation requirements outlined in this manual (See Article 414). Issuing LEs must be attached to the command or unit they will be servicing with COMSEC material. Deviations from this policy must be authorized, in writing, by NCMS N5.

A unit/command/activity shall not receive material under more than one EKMS account. There are only two allowable exceptions to this policy, see Article 166 below.

LEs share the same EKMS ID as the parent account to which they are registered.

166. LOCAL ELEMENT (LE) *IN TRANSIT:* A LE In Transit is a LE unit that is physically remote from its *local* EKMS account and therefore unable to receive routine CMS service from it. LEs In Transit fall into one of two categories:

- A LE unit that will be away from its local EKMS account for more than 45 days and that is proceeding from the location or vicinity of one EKMS account command to the location of or vicinity of another EKMS account command. There are many reasons for such a change of physical location, most often involving deployment, return from deployment, reassignment, training or exercises.

- A ***deployable element*** because it routinely transits from one location to the next and must, therefore, draw needed COMSEC material from a local EKMS account at the base or location where it is operating from temporarily. For example, the EKMS Account of a station or base normally provides CMS service to aircraft squadrons which are attached as LEs. The 45-plus-day criterion **does not apply to *deployable* LEs.**

All such temporary material support relationships must be spelled out in writing in Letters of Agreement or Memorandums of Understanding between the supporting and receiving commands/units. The LOAs/MOUs must clearly delineate the responsibilities of all parties concerned regarding all COMSEC materials involved. A sample LOA which contains the minimum required content can be found in Annex L herein.

167. LMD-ONLY ACCOUNT: LMD-only accounts are equipped with an LMD because they routinely receive fairly large quantities of physical COMSEC material for further issue to LEs. The LMD (running LCMS) assists the EKMS Manager by automating the management of the materials they hold in support of others. LMD-only accounts are **not** capable of receiving electronic key via the EKMS.

170. EKMS CLERK: An EKMS Clerk assists the EKMS Manager and Alternate(s) with routine administrative account matters. Appointment of an EKMS Clerk is not mandatory, but is at the discretion of the CO. If appointed, the individual must be designated in writing by the CO.

Contractors as EKMS Clerks: Contractor personnel may be appointed as account clerks provided they meet the designation requirements of this manual for the position and supervised by the EKMS Manager(s). Close supervision is a necessary condition of the appointment of contractors as clerks.

Access to the LMD/KP: As stipulated in the Security Doctrine for the LMD/KP, access to the LMD/KP is restricted to personnel who have received formal training and are assigned as an EKMS Manager and/or Alternate.

175. EKMS WITNESS: A properly cleared individual (includes contractor personnel) may be called upon to assist a Manager or Local Element in performing routine administrative tasks related to the handling of COMSEC material providing they meet the designation requirements of this manual for the position, and providing they are overseen/supervised by the EKMS Manager(s). An EKMS witness must be authorized access to keying material in writing.

180. KEY MANAGEMENT ENTITIES (KME): Any activity, organization, or person(s) performing some type of key management-related function or functions, which has been assigned an EKMS ID.

182. PRIVILEGE CERTIFICATE MANAGER (PCM): The EKMS ID authorized to create the Privilege Certificate for a KME. The EKMS ID of the PCM will be included in the Privilege Certificate and in the PCM field of the associated Message Signature Key (MSK).

183. FIREFLY POINT OF CONTACT: NCMS is the FIREFLY POC for modern key privileges. Accounts requiring replacement KP FIREFLY (FF) Vector material must contact/order such through NCMS.

184. COMMAND AUTHORITY (CMDAUTH): Individual responsible for managing modern key assets for a department, agency, or command.

Responsibilities include the appointment of User Reps (URs) and associated key ordering privileges.

186. USER REPRESENTATIVE (UR): A KME authorized by an organization and appointed by their responsible Command Authority to order modern key (e.g., MSK, Secure Data Network Device (SDNS), or STE keying material).

188. ORDERING PRIVILEGE MANAGER (OPM): A KME who manages ordering privileges in EKMS and is authorized to designate other KMEs as Short Title Assignment Requestor (STAR) and/or OPM.

190. SHORT TITLE ASSIGNMENT REQUESTOR (STAR): A KME is authorized to request assignment of a new short title and generation of key against that short title. STAR privileges must be registered at the generating account.

192. AUTHORIZED ID: A KME authorized to order against a short title. Authorized IDs are associated with each short title. An Authorized ID can also modify the Distribution Profile for an associated short title.

194. FIREFLY CREDENTIALS MANAGER: A KME responsible for removing outdated credentials from the Directory Service. The Central Facility Finksburg performs this functionality.

CHAPTER 2 -- INTRODUCTION TO COMSEC MATERIAL

FIGURES:

CHAPTER 2 - INTRODUCTION TO COMSEC MATERIAL

201. GENERAL.

a. COMSEC material must be handled and safeguarded based on its assigned classification and accounted for based on its accountability legend (AL) code.

b. COMSEC material control within the U.S. Government is based on a system of centralized and local accounting and decentralized custody and protection. COMSEC material is centrally accountable to the COR and/or accounted for locally at the account command.

c. COMSEC material enters the DON CMCS when:

(1) NSA produces and transfers keying material to DON EKMS accounts for use or distribution (e.g., by United States National Distribution Authority (USNDA)).

(2) A possession report is submitted for COMSEC material that is in the possession of an EKMS Manager but is not charged to the account (e.g., found COMSEC material).

(3) Material that is received by a DON EKMS Manager from another department, agency, foreign government, international organization, or other non-Navy COMSEC accounts (i.e., equipment received from a civilian firm).

205. APPLICATION OF PROCEDURES: Proper and conscientious application of the procedures contained in this publication are intended to provide maximum flexibility, yet ensure proper security and accountability to prevent the loss of COMSEC material and the possible compromise of the information it protects.

210. LIMITATIONS: This publication cannot address every conceivable situation that might arise in the daily handling of COMSEC material. When unusual situations confront a Manager or LE of COMSEC material, the basic tenets applicable to the protection of classified information should be implemented until definitive guidance is provided by NCMS or other authoritative source (e.g., material's CONAUTH, Combatant Commander, ISIC).

215. CONTROL AND REPORTING: Control of COMSEC material is based on the following:

a. A continuous chain of custody receipts using both transfer reports and local custody documents.

b. Accounting records, such as periodic inventory reports, possession reports, generation reports, conversion reports, destruction records, transfer reports, and local custody records.

c. Immediate reporting of COMSEC material incidents to ensure compromise decisions are made expeditiously by controlling/evaluating authorities.

220. COMSEC MATERIAL CLASSIFICATION:

The classification of COMSEC material is indicated by the standard classification markings: TOP SECRET (TS), SECRET (S), CONFIDENTIAL (C), or UNCLASSIFIED (U). The security classification assigned to COMSEC material determines its storage and access requirements.

225. COMSEC MATERIAL IDENTIFICATION:

a. SHORT TITLE: An identifying combination of letters and/or digits (e.g., KG 84A, USKAT 2333) assigned to certain COMSEC material to facilitate accounting and control. A short title consists of 24 alphanumeric characters without special characters, e.g., /, -, etc. The edition field consists of 6 alphanumeric characters.

b. ACCOUNTING (serial/register) NUMBER: Most COMSEC material is assigned an accounting (serial/register) number at the point of origin to facilitate accounting and/or inventory functions. Within LCMS, electronically generated keying material can be assigned an accounting number of "0". Only electronic keying material designated as "copy none, move once" has an accounting number.

SHORT TITLE EXAMPLE: USKAT D 2333 BC 18

Short title:	USKAT D 2333
Edition:	BC
Serial:	18

c. Figure 2-1 contains information and a chart that can be used to determine the meaning of the two-letter digraph that precedes the short title and appears on segmented keying material packaged in canisters. This information also appears on the back of the CMS 25 (Form) in Chapter 7 (Figure 7-1). Short titles are created and defined based on guidance found in CNSSI-4033.

230. ACCOUNTABILITY LEGEND (AL) CODES:

a. Accountability Legend (AL) codes determine how COMSEC material is accounted for within the CMCS. 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:

(1) AL codes assigned to traditional hardcopy COMSEC material:

(a) AL Code 1: COMSEC material is continuously accountable **to the COR** by accounting (serial/register) number from production to destruction.

(b) AL Code 2: COMSEC material is continuously accountable **to the COR** by quantity from production to destruction.

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

(2) AL codes assigned to electronically generated key:

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

(b) AL Code 7: COMSEC material that is electronically generated and **locally accountable** to the generating facility.

NOTE: Electronic key generated under the provisions of NAG 16 (series) (i.e., using KVGs) other than the KP (KOK-22) is not assigned an AL code.

b. CMIO Norfolk is required to continuously account to the COR for all AL Code 4 material. Consequently, **all** transfers of AL Code 4 material **to or from** a CMIO or a non-DON account must be reported to the COR.

c. AL codes are assigned by the originating government department or agency that produces the COMSEC material and represent the minimum accounting standard.

d. AL codes will appear on all accounting reports but not necessarily on the material.

e. The classification of COMSEC material has no bearing on the AL code assigned to it. For example, TOP SECRET COMSEC material may be assigned AL Code 1; however, there is also SECRET, CONFIDENTIAL, and UNCLASSIFIED COMSEC material that is assigned AL Code 1. AL codes determine how material is accounted for and classification determines handling and storage requirements.

f. COMSEC-related items (i.e., items that are not accountable within the CMCS and, consequently, are not assigned an AL Code) are to be handled and safeguarded based on their assigned classification. EKMS 1 (series) and EKMS 5 (series) are examples of such COMSEC-related items.

NOTES: 1. SECNAV M5510.36 (series) defines handling and accounting requirements for classified information and SECNAVINST 5720.42 (series) for FOUO and unclassified information within the DON.

2. COMDTINST M5510.23 (series) contains information for the proper and effective classification, safeguarding and accounting of other classified information.

235. IDENTIFICATION AND AL CODE ASSIGNMENTS FOR ELECTRONIC KEYS CONVERTED FROM PHYSICAL KEYS:

a. Copies of physical key received and subsequently imported into a LMD/KP will be assigned an electronic short title (e.g., USKAT 166 would become USKAD 166) and AL Code that reflects its conversion to electronic form. AL Code 1 must become AL code 6 and AL code 4 must become AL code 7. Additionally, importing key into a LMD/KP for transfer ***outside*** the account command is a form of material reproduction and requires CONAUTH approval. See Article 740 and Annex T for reporting requirements when importing key into LCMS.

b. Physical key loaded directly into a FD using a KOI-18 (not to be loaded in a KP) will retain its original short title. See Article 769.g. for the minimum accounting requirements.

236. CRYPTO MARKING/DESIGNATION:

The marking or designator "CRYPTO" identifies all COMSEC keying material that is used to protect or authenticate classified or sensitive unclassified government or government-derived information, the loss of which could adversely affect national security. The marking "CRYPTO" is not a security classification but a caveat.

237. IDENTIFICATION AND AL CODE ASSIGNMENTS FOR REMOVABLE MEDIA STORING ELECTRONIC KEYS:

a. Any physical media that is to be transferred or issued, other than a KSD-64A, on which electronic keys have been loaded will have a short title and an AL code of 1 or 4. In the case of Tier 0-provided media, encryption, classification, etc. will be factors in the AL Code assignment.

b. See Article 769.i. for guidance on assigning short titles, AL Codes and classification to locally provided media storing electronic keys.

238. SYSTEM KEYS FOR LCMS:

a. EKMS Message keys.

(1) KP FIREFLY Key - A modern (asymmetric) key used to create FIREFLY vectors (credentials) to encrypt keying material for distribution between EKMS accounts or to perform benign fill techniques.

(2) Message Signature Key (MSK) - The EKMS MSK is a modern key generated by the EKMS CF and filled from a KSD-64A cryptographically “sign” EKMS messages.

(a) FIREFLY Key and MSK along with the KP Privilege Certificate (PRIV CERT) must be requested from the NCMS whenever an LMD/KP is brought on-line for the first time (site initialization) or following a catastrophic failure of the LMD/KP that results in the system requiring a new site initialization. Commands should contact NCMS//N3 only if experiencing difficulties obtaining requested key in a timely manner and need NCMS intervention to resolve.

(b) The request for these keys and PRIV CERT is NOT required when a KP is being replaced for routine recertification or for some other event not resulting in catastrophic failure of the LMD/KP.

(c) To obtain either a new FIREFLY Vector Set or Message Signature Key, see Article 670.

(d) Once both the KP FIREFLY Key and MSK have been loaded in the KOK-22A, a LCMS backup must be performed and both the KP FIREFLY Key and MSK must be recorded as destroyed using the "filled in end equipment" function within LCMS. The associated KSD-64As can be zeroized using the KOK-22A. Failure to record these items, as destroyed NLT the 5th working day of the month following their use must be documented as a non-reportable PDS in accordance with Chapter 10. Procedures for loading of either the FF Vector Set or MSK are outlined in EKMS-704(series) (L3 Communications) ~~pages 9-9 through 9-12~~.

AMD-9

NOTE: The procedures in 238.a.2.d above is not applicable to test FF Vector Sets or MSKs held/used by~~ CMS A&A Training Teams and ~~CID Learning Sites. These short titles are: KTU 202 874055 and KTU 4294967297 874055, respectively.

b. KP Internal keys - There are several keys that the KP generates and uses internally which the user never encounters directly, but are affected by certain LMD/KP functions/processes. These functions/processes are: Site Reinitialization, Changeover, and KP Rekey and each are discussed below.

(1) **Site Reinitialization** - Enables the recovery of all protected data stored on the LMD and is used when a KP must be replaced with a new KP due to failure or recertification. The REINIT keys are used during this process and KP User Keys are recreated. Step-by-step procedures can be found in EKMS-704 (series). To ensure consistency of LCMS Activity Data for tracking changeover (described below), accounts will perform KP changeover and backup following a KP Site Reinitialization.

(2) **Changeover** - The process used to re-encrypt the LMD database when the cryptoperiod of the Key Encryption Key Local (KEKL) expires. The KEKL has a cryptoperiod of three months. At a minimum, KP Changeover will be performed following a Site Reinitialization (as discussed above) and at a minimum of every three months thereafter (**maximum 92 days between changeovers**). It is understood that larger accounts may have to perform Changeover more frequently and doing so will reduce the time the

process takes for subsequent changeovers minimizing non-availability of the KP for account functions.

Although supersession and re-encryption of the LMD/KP database is a system function, an operator must initiate this action by performing a Changeover as outlined in EKMS 704(series).

The process of re-encryption and supersession is a background operation of the LMD/KP and must be initiated manually. The key that is produced during this process is the **NAVREINIT 2** key.

(3) REINIT 1 and NAVREINIT 2 keys created during Site Initialization, Site Reinitialization and/or subsequent Changeover processes, as applicable must be accounted for within the CMCS and LCMS. The KSD-64As will be protected in accordance with Article 1185.

(4) **KP Rekey** - The process by which the EKMS Manager requests an update to the FIREFLY Key is required to be conducted at a minimum of annually. The KP Rekey Request is required to prevent interruption of service with the EKMS CF and the COR. (Both entities will ship electronic keys to an account and must have current credentials.) Procedures to request the KP Rekey are contained in EKMS 704 (series). There is no physical key required for this process. **Deployable units that will be deployed when the current FIREFLY key supersedes are strongly encouraged to perform a KP rekey prior to deployment.**

NOTE: Before conducting a KP rekey and posting new credentials, all Bulk Encrypted Transactions (BETs) must be processed.

c. User Keys - Consists of the System Administrator (SYSADMN) and System Operator (SYSOPR), which are produced by the LMD/KP when requesting to add either function. The EKMS Manager manually initiates SYSADMN and SYSOPR keys.

d. KG Rules: KG Rules (Short Title: USKAD BU71260 880091) are produced and distributed by DIRNSA electronically to EKMS accounts. The KG Rules are designed to enable to KOK-22A (KP) to locally produce keying material for existing and emerging COMSEC equipment. EKMS Managers must load the latest version of KG Rules within 30 days of receipt. The previous version must be destroyed NLT the 5th working day of the month following the month of loading the new version. Failure to destroy previous KG Rules within the timeframe set forth in this article constitutes a COMSEC Incident (Late destruction). Procedures for loading the KG Rules can be found in the EKMS-704 (series).

NOTE: The provisions of 238.b above are NOT applicable to TESTPAC KPs.

240. CONTROLLED CRYPTOGRAPHIC ITEM (CCI):

Controlled Cryptographic Item (CCI) is the designator which identifies secure telecommunications or information handling equipment, or an associated cryptographic component, which is unclassified but controlled within the CMCS.

245. STATUS OF COMSEC MATERIAL:

a. The authorized period of use for COMSEC material is defined by its status (i.e., one of three possible conditions). Status for COMSEC material is assigned at the direction of the CONAUTH or originator of the material.

b. The status for equipment and non-keying material items is changed infrequently as they are used for extended periods of time. This material is in effect until it is replaced or superseded.

c. The status for COMSEC keying material is promulgated repeatedly as its lifespan can vary from hours to an indefinite period of time. Most keying material is superseded on a regular basis due to operational use. COMSEC keying material will, at all times, be in one of three status conditions:

(1) Reserve: Held for future use. (See Note 2 below).

(2) Effective: Authorized for use.

(3) Superseded: No longer authorized for use; must be destroyed within the time frames in Article 540.

NOTES: 1. An edition of COMSEC keying material is one in a series of printings of the same short title. Each edition has its own effective period and may contain different key variables divided into parts, known as segments. Each segment within an edition will have a designated effective period (i.e., daily, weekly, monthly, quarterly, etc.) assigned to it based on the key's

crypto-equipment. This effective period is commonly known as the segment's cryptoperiod.

2. Some keying material (e.g., Inter-Theater COMSEC Package (ICP)) may be categorized as being in a contingency status. Material in this category is defined as material held for use under specific operational conditions or in support of specific contingency plans. Status documents (e.g., SCMR) will reflect this material as when directed (WHENDI).

250. COMSEC MATERIAL SUPERSESSION:

Supersession refers to a time when a particular item of COMSEC material is no longer eligible for use. COMSEC material is superseded in one of three ways:

a. **Regular supersession**: Supersession which is based on a specific, pre-determined supersession date for each edition of material by the Controlling Authority. For example, each edition of a monthly key tape is superseded on the first day of the month after its implementation; each edition of ten-day material is superseded on the 11th, 21st, and the 31st of the month.

b. **Irregular supersession**: Supersession that is not pre-determined but which occurs as a result of use. Editions and individual segments of irregularly superseded COMSEC material are to be destroyed after the material has been used operationally, when the CONAUTH directs supersession, or, in the case of maintenance key, it may be used until the key becomes unserviceable. Irregular supersession is normally associated with one-time pads, test key, maintenance key, publications, and equipment.

c. **Emergency supersession**: An unplanned change of supersession, usually as the result of a compromise directed by the Controlling Authority.

255. SOURCES OF SUPERSESSION INFORMATION:

The supersession or status of COMSEC material held by EKMS accounts can be determined using the following sources:

(1) **STATUS OF COMSEC MATERIAL REPORT (SCMR)**: The SCMR which is classified SECRET (NOFORN) is updated by the COR on a monthly basis and contains a composite listing of most COMSEC

material distributed to DON EKMS accounts.

(2) This report is sent automatically to the mailbox for each DON EKMS account via the X.400 Message Server.

(3) Annex E contains a portion of a typical page of a SCMR and a brief explanation of the data contained in it.

NOTE: In the event of status information conflicts, EKMS Managers must use the most recent information available as promulgated by the Controlling Authority or contact NCMS (N3)for guidance.

(4) Editions of keying material produced in electronic form have the same effective and supersession dates as that of the physical version of the material. Example: USKAD 2099 edition C and USKAT 2099 edition C have the same effective and supersession dates. Accordingly both of the items cited in the example should be on the same end-of-the-month destruction report. EKMS Managers are encouraged to verify at a minimum of monthly, or more frequently when material is emergency superseded or more recent information is promulgated by message traffic and prior to end-of-the-month destruction the status information contained in LCMS as status information is frequently changed as a result of emergency supersession.

a. **AMSG-600**: AMSG-600 contains status information for NATO COMSEC material, takes precedence over the SCMR and must be held by DON accounts which hold NATO material.

b. **Joint COMSEC Management Office (JCMO) MacDill AFB, FL**: Status information for keying material designated for use as part of the Inter-Theater COMSEC Package (ICP) is promulgated in a series of messages using pre-determined date-time-groups (DTGs) by the JCMO on a quarterly basis. Status and other information related to JCMO Short Titles can be found at: https://vela.stratcom.smil.mil/restrict/jcmo.

	DTG	**AIG**	**SUBJ**
(1)	211600Z	7862/3	Conventional package..
(2)	211602Z	901	SOC package...........
(3)	211603Z	7092	TAC/STRAT.............
(4)	211604Z	902	TRI-TAC...............
(5)	211605Z	906	KG-84/KIV-7...........
(6)	211606Z	7094	USKAT-1949............
(7)	211607Z	8721	JTAO package..........
(8)	211610Z		USCENTCOM AOR JICP Usage

(9)	211611Z	8709	IFF/DAMA package......
(10)	211612Z	904	Subsurface Fleet......
(11)	211613Z	903	Weather KEYMAT........
(12)	261614Z		Mode 4 and 5 IFF .....
(13)	211615Z	7093	JCS Emergency ....
(14)	211616Z	7862/3	Supersession Source...
(15)	211617Z	8711	GBS ....
(16)	211618Z		CENTRIXS KEYMAT (GCTF)
(17)	211619Z		CENTRIXS KEYMAT (XNET)

c. **CJCSI 3260.01(series):** A limited number of commands are authorized to hold two-person controlled (TPC) Sealed Authentication Systems (SAS) keying material.

(1) Policy and procedures for handling TPC/SAS material are contained in CJCSI 3260.01(series). The COR's role for TPC or SAS material is limited to accounting functions only (tracking movement and reconciliation of inventories). Click here for contact data, to obtain, if required.

(2) Status information for SAS material is promulgated by JCS message and is not listed on the SCMR. Type Commanders also promulgate status information for SAS material. For example, COMSUBPAC and COMSUBLANT disseminate a monthly message to the collective address designator (CAD); "SUBPAC" and "SUBLANT," which list the latest SAS related messages promulgated by theater Commanders.

d. **General Message from CONAUTH**. Status information is also promulgated by CONAUTHs via GENERAL messages (e.g., ALCOM, ALCOMPAC P, ALCOMLANT A).

NOTE: Effective ALCOM, ALCOMLANT A, and ALCOMPAC P messages can be obtained at the respective URLs discussed in the document referred to in Annex D.

e. **COAST GUARD (COGARD) C4ITSC Joint Inter-Agency Counterdrug COMSEC (JIACC) KEYMAT Package Monthly Information and Status Message**. Status information for keying material contained in this package is promulgated by GENSER message using a fixed date-time-group of 181800Z MMM YY. The monthly message is transmitted to AIG 11901. Status information and other pertinent information concerning the package or other CG controlled short titles can be found at www.uscg.smil.mil/sites/C4IT/COMSEC/default.aspx.

f. **COMSEC Publications and Manuals**: The status of

COMSEC manuals and publications is normally listed on the Letter of Promulgation (LOP) page within these documents. When not listed, the originator of the document promulgates status via separate correspondence.

g. **AL CODE 6 and 7 COMSEC Material**: The generating facility of AL Code 6 and 7 material must assign the status of all material it generates as dictated by the CONAUTH.

260. CATEGORIES OF COMSEC MATERIAL:

COMSEC material consists of a variety of products used to secure telecommunications or ensure the authenticity of such communications. COMSEC material includes, but is not limited to COMSEC key, items that embody or describe COMSEC logic, and other items that perform COMSEC functions. COMSEC material is divided into three categories or material types: keying material, equipment, and COMSEC Aids.

a. **Keying Material**: A type of COMSEC material that supplies either encoding means for manual and auto-manual cryptosystems or key for machine cryptosystems. Keying material may or may not be marked or designated "CRYPTO." Keying material includes both Paper-Mylar-Paper (PMP) and paper (which may be extractable or non-extractable), electronic, e.g. KP produced key, keying material on magnetic media, and other non-paper items (which maybe extractable or non-extractable).

(1) Paper keying material includes keylists, codes, authenticators, Identify Friend or Foe (IFF) keying material, and one-time pads, **but does not include canister-packaged key tapes**. Keying material can be designated for use as operational, exercise, test (on-the-air), maintenance (off-the-air), or training (off-the-air e.g., classroom). Examples of Short Titles associated with paper keying material is illustrated below:

Keylists	(AKAK/USKAK)
Codes	(AKAC/USKAC)
Authenticators	(AKAA/USKAA)
One-time Pads	(AKAP/USKAP)

NOTE: Although the above examples illustrate paper COMSEC material with both regular and/or irregular supersession, these items MUST be registered in LCMS as “AIDES”. Registration of these items in LCMS as "Traditional" will cause problems during the reconciliation of subsequent

editions."

(a) Extractable keying material is designed to permit the extraction and removal of individual segments of key for hourly, daily, weekly, etc... use. Individual segments are indicated by perforations, dotted lines, or similar separations to permit removal. Examples of extractable keying material are key tapes, and authentication systems consisting of hourly or daily authentication tables.

NOTE: Although listed as extractable keying material, canister-packaged keying material is not paper COMSEC material.

(b) Non-extractable keying material is designed to remain intact throughout its entire effective period. An example of non-extractable keying material is operations or numeral codes with separate encode and decode sections.

NOTE: Extractable/non-extractable as described above refers to the physical condition of paper keying material and not the physical or electronic removal or extraction of key from a device.

(2) Electronic keying material includes electronically generated key, either produced by a KP or other key variable generating device, electronic keys converted from key tape, electronic keys stored on magnetic media (e.g., floppy disk) and key loaded onto a fill device (e.g., KSD 64A).

(3) Non-paper keying material includes, key tapes, keying plugs, keyed microcircuits, removable media (e.g., floppy disks), magnetic tapes, and keying material in solid state form such as programmable read-only memories (PROMs), read-only memories (ROMs), metallic oxide semi-conductor (MOS) chips, and micro-miniature tamper protection systems (micro-TPS).

b. **COMSEC Equipment**: Equipment designed to provide security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor and subsequently by reconverting such information to its original form for authorized recipients, as well as equipment designed specifically to aid in, or act as an essential element of the conversion process. NAVREINIT 2 keys must also be registered as equipment in LCMS.

c. **COMSEC Aides (otherwise known as COMSEC-Related**

Information): KAMs, KAOs, call signs, frequency systems, REINIT 1 CIKS, and miscellaneous material not listed above.

NOTES: 1. Selected limited maintenance KAMs are being/have been replaced by limited maintenance manuals (LMMs). LMMs are unclassified and are not accountable as COMSEC or COMSEC-related material.

2. Status information for LMMs will be promulgated by NCMS (N3).

3. LMMs will have both a Technical Manual Identification Number (TMIN) and a National Stock Number (NSN) assigned to them. LMMs may be requested from:

**Aviation Supply Officer
Naval Publications and Forms Directorates
5801 Tabor Avenue (Code 1013)
Philadelphia, PA 19120-5099**

DIGRAPHS ON SEGMENTED KEYING MATERIAL PACKAGED IN CANISTERS

1. **General**: COMSEC keying material packaged in canisters has a preprinted digraph, consisting of two letters, printed to the left of the short title (e.g., "AA" USKAT 1000 BG 1234) on each extractable segment of the tape leader. The two letters are read left to right and provide the following information:

a. **First letter**: Identifies the number of different key settings within the canister, the number of copies of each key setting, and the total number of segments in the canister, respectively.

b. **Second letter**: Identifies the cryptoperiod.

2. Use Figure 2-1 to determine the meaning of the digraph appearing on U.S.-produced keying material packaged in canisters. Use Figure 2-2 to determine the meaning of the digraph appearing on British-produced keying material packaged in canisters.

DIGRAPH CODES ASSIGNED TO U.S.-PRODUCED KEY

1ST LETTER

		COPIES	TOTAL
	KEYS	OF KEYS	SEGMENTS
A.	31	1	31
B.	5	3	15
C.	1	5	5
D.	6	5	30
E.	5	1	5
F.	1	10	10
G.	16	1	16
H.	1	31	31
I.	1	15	15
J.	26	1	26
K.	6	12	72
L.	35	1	35
M.	2	1	2
N.	Contact CONAUTH		
O.	68	1	68[*]
P.	1	45	45
Q.	34	1	34
R.	4	5	20
S.	75	1	75
T.	12	1	12
U.	65	1	65
V.	62	1	62
W.	1	65	65
Y.	26	2	52
Z.	15	5	75

2ND LETTER

A.	Daily (24 hours)
B.	Weekly (7 days)
C.	Monthly
D.	Special mission; not to exceed 24 hours
E.	No prescribed cryptoperiod
F.	Three months
G.	Yearly
H.	Contact Controlling Authority
I.	Six months
J.	Monthly beginning on 1st day used

FIGURE 2-1

[*] The digraph OA was assigned by DIRNSA exclusively for AKAT 3662. This digraph will not be printed on or used with any other keying material. Segment usage is outlined in the Joint Staff ICP monthly status messages (211600Z).

DIGRAPH CODES ASSIGNED TO BRITISH-PRODUCED KEY

1ST LETTER

		COPIES	TOTAL
	KEYS	OF KEYS	SEGMENTS
A.	31	1	31
B.	5	3	15
C.	1	5	5
D.	6	5	30
E.	5	1	5
F.	1	10	10
G.	16	1	16
H.	1	31	31
I.	1	15	15
K.	6	1	6
L.	35	1	35
M.	2	1	2
N.	Contact CONAUTH		
P.	20	2	40
Q.	34	1	34
R.	15	2	30
S.	75	1	75
T.	12	1	12
U.	65	1	65
V.	62	1	62
W.	1	65	65
X.	20	1	20
Y.	30	1	30

2ND LETTER

A.	Daily (24 hours)
B.	Weekly (7 days)
C.	Monthly
D.	Special mission; not to exceed 24 hours
E.	No prescribed cryptoperiod
F.	Three months
G.	Yearly
H.	Contact Controlling Authority
I.	Six months
J.	Bi-monthly

FIGURE 2-2

CHAPTER 3 -- CMS EDUCATION, TRAINING, AND AUDITS

CHAPTER 3 - CMS EDUCATION, TRAINING, AND AUDITS

301. GENERAL:

a. COR Audit Team personnel should be viewed as an EKMS Manager's right-hand asset. Their training and experience provide a readily available source of technical expertise in all areas related to COMSEC material. Their charter "to train and assist" should be used advantageously at every opportunity by every command handling COMSEC material.

b. Education and training services are available worldwide to provide basic skills required to fulfill the responsibilities of an EKMS Manager and to assist/train personnel in the procedures required to properly manage an EKMS account. Prospective EKMS Managers receive their core training by attending and satisfactorily completing the Navy Electronic Key Management System (EKMS) Course of Instruction (COI). COR Audit Teams are available, on request, to provide follow-on or supplemental training as may be required.

305. NAVY EKMS MANAGER COURSE OF INSTRUCTION (COI):

a. General: The Navy EKMS Manager COI is a 15-day course that provides the basic skills required to fill an EKMS Manager/Primary Alternate position. It emphasizes COMSEC accounting and reporting requirements, and the use of the Local Management Device (LMD) KOK-22A (KP) to manage COMSEC material and support the generation, encryption, decryption, inventory and destruction of electronic key. This course is a pre-requisite for the EKMS Manager PQS and completion of the COI does not imply completion of the PQS is not required unless otherwise stated in Article 312.

b. Locations: The Navy EKMS Manager COI is offered in the following areas:

(1) CONUS East Coast:

(a) Naval Submarine School, Groton, CT
(b) Fleet Training Center, Norfolk, VA
(c) Trident Training Facility, Kings Bay, GA
(d) Fleet Training Center, Mayport, FL
(e) USMC II MEF MCMO, Camp Lejeune, NC

(2) CONUS West Coast:
(a) Trident Training Facility, Bangor, WA

(b) Training Support Center San Diego, CA
(c) USMC I MEF MCMO, Camp Pendleton, CA

(3) EUROPE: Naval Computer and Telecommunications Area Master Station Europe Central, Naples, Italy.

(4) PACIFIC:

(a) Afloat Training Group, Middle Pacific (MIDPAC) Pearl Harbor, HI
(b) Training Support Detachment (TSD) Western Pacific, Yokosuka, Japan
(c) USMC III MEF MCMO, Okinawa, Japan

c. Quotas: Quota control for the Navy EKMS Manager COI is managed by each individual training site. Information on class schedules can be found in the Catalog of Non-resident Training Courses (CANTRAC) at: https://www.netc.navy.mil/Development.aspx.

NOTE: USCG EKMS Accounts must coordinate quota requests with their respective ISIC AND COGARD C4ITSC prior to submission of Electronic Training Requests (ETR).

d. School House Addresses/Telephone Numbers:

(1) Groton, CT:

CENTER FOR INFORMATION DOMINANCE
LEARNING SITE GROTON
BOX 700
BLDG 518 ROOM 418
ATTN: EKMS COI
GROTON, CT 06349-5700

PLA: CENINFODOM LS GROTON CT//CID//
DSN: 694-3114 COMM: (860) 694-3114

(2) Virginia Beach, VA:

CID LEARNING SITE NORFOLK
1887 VIKING DRIVE
CHAMBERLAIN HALL BLDG 102
ATTN: EKMS COI
VIRGINIA BEACH, VA 23461

PLA: CENINFODOM LS NORFOLK
DSN: 492-6289/6296 COMM: (757) 492-6289

(3) Kings Bay, GA:

CID LEARNING SITE KINGS BAY
TRIDENT TRAINING FACILITY
1040 USS GEORGIA AVE
(BLDG 1065)
KINGS BAY GA 31547-2610

PLA: TRITRAFAC KINGS BAY GA//42//
DSN: 573-8167 COMM: (912)573-8167

(4) Mayport, FL:

COMMANDING OFFICER
FLEET TRAINING CENTER MAYPORT
BLDG 351 BALTIMORE STREET
ATTN: EKMS COI
MAYPORT FL 32228-0147

PLA: FLETRACEN MAYPORT FL//N3//
DSN: 922-5239 COMM: (904) 270-5239

(5) Bangor, WA:

CID LEARNING SITE BANGOR
ATTN: EKMS SCHOOLHOUSE
2000 THRESHER AVENUE
ATTN: EKMS COI
SILVERDALE WA 98315-2000

PLA: TRITRAFAC BANGOR WA//42//
DSN: 322-2688 COMM: (360) 315-2688

(6) San Diego, CA:

COMMANDING OFFICER
TRAINING SUPPORT CENTER SAN DIEGO
ATTN: EKMS COI
3975 NORMAN SCOTT RD SUITE 1
SAN DIEGO CA 92136-5588

PLA: TRASUPPCEN SAN DIEGO CA//76//
DSN: 526-7061 COMM: (619) 556-7061

(7) Pearl Harbor, HI:
CID LEARNING SITE HAWAII

ATTN: EKMS COI
1130 BOLE LOOP
PEARL HARBOR HI 96860

PLA: CENINFODOM LS PEARL HARBOR HI
DSN: 472-0560 COMM: (808)472-0560

(8) Yokosuka, JA:

COMMANDING OFFICER
TRAINING SUPPORT DETACHMENT WEST PAC
PSC 473 BOX 16
ATTN: EKMS COI
FPO AP 96349-0052

EMAIL: quota@atgwp.navy.mil

PLA: AFLOATRAGRUWESTPAC YOKOSUKA JA//20//
DSN: 243-3383 COMM: 011-81-311-243-3383

(9) Camp Lejeune, NC:

USMC II MARINE EXPEDITIONARY FORCE MCMO
BLDG H-17 SOUTH
CAMP LEJEUNE NC 28542-0080

PLA: USMC II MEF//G6/MCMO//
DSN: 751-7093/6724 COMM: (910) 451-7093/6724

(10) Camp Courtney, JA:

COMMANDING GENERAL
ATTN G6 MCMO
III MEF
UNIT 35601
FPO AP 96606 5601

PLA: USMC III MEF//G6//
DSN: 622-7850 COMM: 011-81-611-722-7850 (MCMO DIRECTOR)
DSN: 622-9306 COMM: 011-81-611-722-9306 (MCMO CHIEF)
DSN: 622-7845 COMM: 011-81-611-722-7845 (MCMO OPS CHIEF)
DSN: 622-7262 COMM: 011-81-611-722-7262 (NON-SECURE FAX)

(11) Camp Pendleton, CA:

COMMANDING GENERAL
I MEF G-6
ATTN: EKMS
BLDG. 210722, ROOM 116
C STREET
CAMP PENDLETON, CA 92055-5325

PLA: USMC I MEF//G6//
DSN: 365-9137 COMM: (760)725-9137

e. Criteria for Attending: Criteria for attending the Navy EKMS Manager COI are:

(1) U.S. citizenship (includes naturalized)
(2) SECRET or higher security clearance
(3) E-5/GS-5/(NSPS/DCIPS Pay Band 1) or above
(4) Six months of government service
(5) Be assigned to or designated to fill an EKMS Account Manager, Alternate, or EKMS Inspector billet.

f. Recommendations for improving the course curriculum should be forwarded to:

Mailing Addresses: (1) CENTER FOR INFORMATION DOMINANCE
640 ROBERT AVE
PENSACOLA FL 32511-5138

Phone number: (1) (850) 452-6111
DSN: 522-6111

312. PERSONNEL QUALIFICATION STANDARDS (PQS):

a. 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. The PQS is available from https://www.netc.navy.mil/development.aspx

NOTE: The EKMS PQS is not intended to replace formal classroom training. The PQS is intended to supplement, through hands-on training at the unit level the classroom training required by EKMS Managers and Alternate EKMS

Managers. While not mandated herein, the applicability of PQS or other local training avenues for civilian employees whose position requires access to COMSEC material will be as promulgated in command, ISIC, or TYCOM training or COMSEC policies and should be clarified in position descriptions or individual performance plans.

315. PRE-AUDIT TRAINING VISITS AND COR AUDITS:

a. Pre-Audit Training Visits: DON CMS accounts have the option to receive a Training Visit from their local CMS COR Audit Team at any time. It is HIGHLY RECOMMENDED and in the command's best interest to take advantage of the training and assistance services prior to an audit, deployment or upon change of command or Manager. NCMS will fund one training visit per audit cycle. The requesting activity may request multiple visits but are responsible for providing funding for training visits or assistance beyond the one (funded by NCMS) as described above.

NOTE: Article 325 contains additional information on COR Audit Team services.

b. COR Audits: All DON EKMS accounts must undergo a formal CMS COR Audit every 24 months. Audits will be conducted in accordance with the procedures contained in EKMS 3 (series).

NOTE: EKMS Managers are required to use the current version of the CMS COR Audit Manual (EKMS 3 (series)) to conduct a semi-annual self-assessment of their account.

320. COR AUDIT TEAMS:

a. COR Audit Teams constitute a worldwide network of COMSEC subject matter experts. They were established to provide assistance and training to personnel assigned COMSEC responsibilities. Training may be conducted at the account command or at the facility of the area COR Audit Team.

b. Specific training topics are scheduled by the Training Team offices at established intervals and cover both general and specific subjects of interest to COs, OICs, SCMSROs, ISICs, CMS COR Auditors, EKMS Managers and LEs.

c. COR Audit Team assistance is limited to COMSEC issues only, and not the operational aspects of communications or cryptology. Specific assistance may be requested by contacting your local COR Audit Team.

325. COR AUDIT TEAM SERVICES:

a. General: COR Audit Teams can provide assistance in resolving general or specific problems and in most cases this can be done over the telephone. When required, a date can be arranged for a Training Team to visit a command.

b. Request for Service(s): Submit a request for service(s) via letter, message, or e-mail to the closest COR Audit Team in your area from Article 330.

c. Types of Services: COR Audit Teams provide the following services:

(1) EKMS TRAINING VISITS:

(a) Training Visits provide the basis for self-improvement and are not to be confused with a formal CMS COR Audit. Training Visits can last from eight hours to several days, dependent upon the size of the activity/account, are strictly informal, and provide guidance on the policy and procedures for COMSEC material. The COR Audit Teams will use a detailed brief/Instructor guide in addition to the EKMS (series) publications. This gives the command a health check of their EKMS account and trains the COMSEC Management Team on any areas where deficiencies are noted.

(b) Results of a Training Team visit will be restricted to NCMS and the activity visited unless otherwise disseminated by the activity visited. A debrief to the Commanding Officer or designated representative and the EKMS Manager is provided within five working days, which covers specific areas of training and the personnel involved.

(c) Pre-audit visits will include the EKMS account and additional LEs as permitted by travel limitations and the operational requirements of the visited activity. For any LE not visited, the EKMS Manager should conduct a review of each using the EKMS-3(series) to ensure proper procedures are being adhered to.

NOTE: Training for LEs must be coordinated and scheduled by the parent EKMS account with the COR Audit Team.

(2) EKMS FOR COMMANDING OFFICERs:

This mandatory training is for COs, SCMSROs, and OICs to enable them to effectively monitor their account's compliance with established procedures. Training lasts approximately two hours and may be conducted at the account's command or other location as coordinated by the requesting command.

(3) CMS COR AUDITOR CERTIFICATION/RECERTIFICATION:

(a) CMS COR Auditor training requirements consist of satisfactory completion of the EKMS COI, the COR Audit Team Training Seminar, observation of 1 CMS COR Audit and conducting 2 CMS COR Audits under the instruction of a certified COR Auditor.

(b) ISICs may recommend personnel to be COR Auditors but NCMS will be the final authority for certification of Auditors.

(c) Personnel that fulfill the requirements of paragraph c.(3)(a) above will be awarded a CMS COR Auditor Certificate. NCMS will mail this certificate to the newly qualified auditor's ISIC.

(d) CMS COR Auditor training is conducted by all COR Audit Teams.

(e) CMS COR Auditors must attend CMS COR Audit Team Training Seminar every 36 months to maintain certification.

NOTE: See Article 315.b and 440.a for additional Information related to audits. Audit criteria for perspective CMS COR Auditors is outlined in EKMS-3(series).

(4) EKMS LE WORKSHOPS:

Provides EKMS Managers with supplemental training for their LEs. This training lasts approximately three hours and can be provided at the account command or at the COR Audit Team site.

(5) EKMS TOWN HALLS:

Addresses changes to COMSEC policy and procedures, recurring problems in account management, insecurity trends and topics of concern introduced by attendees. EKMS Town Halls are hosted annually (funding permitting) by NCMS and are primarily intended for COs, EKMS Inspectors, and EKMS Managers. While attendance at EKMS Town Halls is mandatory for Commanding Officers and EKMS Managers, it is highly recommended that SCMSROs and the Primary Alternate attend as well, when possible. Briefs are available from the servicing COR Audit team for those unable to attend.

(6) SECURE TELEPHONE POLICY BRIEFS:

Provides guidance and training on Secure Telephone policies and procedures including but not limited to the handling and safeguarding of Type I material held by DON EKMS accounts only.

330. AREAS OF RESPONSIBILITY FOR COR AUDIT TEAMS:

COR Audit Team responsibilities are divided among 11 teams, each responsible for a specific geographical region as shown below:

a. ATLANTIC REGION

(1) Washington, DC. Delaware, Maryland, Northern Virginia (including Quantico & Dahlgren), Pennsylvania, and the District of Columbia.

(2) Norfolk, VA. Illinois, Indiana, Iowa, Kansas, Kentucky, Michigan, Minnesota, Missouri, North Carolina (Elizabeth City and Cape Hatteras only), Ohio, Virginia (less Northern Virginia, Dahlgren, and Quantico), West Virginia, and Wisconsin.

(3 Mayport, FL. Alabama, Caribbean (Andros Island Test Range), Florida, Georgia, Guantanamo Bay, Lesser Antilles, Louisiana, Mississippi, Panama, Puerto Rico and Texas.

(4) Groton, CT. Connecticut, Iceland, Maine, Massachusetts, New Hampshire, New Jersey, New York, ~~Pennsylvania~~, Rhode Island, Vermont, and Newfoundland.

(5) Camp Lejeune, NC. Arkansas, North Carolina (less Elizabeth City and Cape Hatteras areas), Oklahoma, South Carolina and Tennessee.

b. **PACIFIC REGION**

(1) Pearl Harbor, HI. Hawaii, Midway Island, All EASTPAC.

(2) Puget Sound, WA. Alaska, Idaho, Montana, Nebraska, North Dakota, Oregon, South Dakota, Washington, and Wyoming.

(3) San Diego, CA. Arizona, California, Colorado, New Mexico, Nevada, and Utah.

(4) Far East Yokosuka, Japan. Japan, Korea, Singapore, Mariana Islands, Philippines, and all WESTPAC/Indian Ocean between 060E and 165E.

(5) Okinawa, Japan. Sasebo, Iwakuni.

c. **EUROPEAN REGION**

(1) Naples, Italy. Europe including the Mediterranean Sea, Indian Ocean (West of 060E), Persian Gulf and United Kingdom.

CHAPTER 4 -- ESTABLISHMENT AND MAINTENANCE OF AN EKMS ACCOUNT AND ASSOCIATED RESPONSIBILITIES

CHAPTER 4 - ESTABLISHMENT AND MAINTENANCE OF AN EKMS ACCOUNT AND ASSOCIATED RESPONSIBILITIES

401. REQUIREMENT FOR AN EKMS ACCOUNT:

An organization that requires COMSEC material must obtain such material through an EKMS COMSEC account managed by a designated EKMS Manager. When it is not possible to draw needed COMSEC material from an existing EKMS account either within the organization or located in close proximity , the requirement to establish a new EKMS account must be validated by the organization's Immediate Superior in Command (ISIC). Commands led by a Flag Officer can self-validate.

405. ESTABLISHING AN EKMS ACCOUNT:

a. **Steps Required to Establish an EKMS account**:

(1) ISIC validates requirement for an EKMS account to approving authority identified in Article 405.e.

(2) ISIC validates command compliance with physical security safeguards for the storage of COMSEC material to approving authority identified in Article 405.e.

(3) ISIC determines the required COMSEC material.

(4) Command/ISIC obtains CONAUTH authorization in accordance with Article 405.c.

(5) CO designates in writing a qualified EKMS Manager and Alternate EKMS Manager(s).

(6) Command submits request for account establishment and required COMSEC material to NCMS.

b. **Preparation**:

(1) Prior to establishing an EKMS account, an organization must coordinate with its ISIC and determine its required COMSEC material holdings. In determining material holdings, HCI information (classification level of material required) must also be considered and included in the request to establish an EKMS account. Article 430 contains additional information.

(2) Additionally, a physical security inspection of the

area(s) being designated for storage of COMSEC material must be conducted to ensure compliance with the minimum physical security requirements for safeguarding COMSEC material. Physical security requirements are contained in Chapter 5 and Annexes M, N, and O.

c. **Validation of Authorized Holdings**:

The distribution of all COMSEC material requires authorization from the CONAUTH of the material. Validation requirements are as follows:

(1) Navy shore units must obtain CONAUTH validation for COMSEC material required by their account.

(2) Navy surface, sub-surface, and Coast Guard surface units do not require CONAUTH validation for COMSEC material contained in the standard fleet allowance instructions (e.g., COMLANTFLT/COMPACFLT/COMUSNAVEURINST C2282.1(series), and Coast Guard area instructions (e.g., COMPACAREAINST C2282.1) and/or messages respectively.

NOTE: ISICs are responsible for obtaining CONAUTH validation for COMSEC material not reflected in fleet instructions as part of the commands standard allowance.

(3) USMC Fleet Marine Forces and all Coast Guard commands must have their COMSEC material holdings validated by the Commander, Marine Force (COMMARFOR) LANT, PAC or RES, or Commander, COGARD C4ITSC, as appropriate.

(4) USMC supporting establishments (e.g., bases, posts, and stations) must have their COMSEC material holdings validated by their ISIC.

d. **Lead Time to Establish**: At least 45 days is required to establish an EKMS account and to provide the initial COMSEC material. Initial issue for afloat units will be provided IAW COMLANTFLT/COMPACFLT/COMUSNAVEURINST C2282.1(series) Ashore units contact ISIC and CONAUTH.

e. **Request to Establish**:

(1) A message must be submitted to NCMS//N31// to establish an EKMS account. COMSEC material will not be distributed without a valid EKMS account number.

(2) Annex G contains a sample request listing all the required data for establishing an EKMS account.

(3) EKMS account establishment request will be addressed as follows:

(a) **Navy and MSC Commands**:

Submit to NCMS WASHINGTON DC//N31//, info ISIC, administrative Chain of Command, CNO WASHINGTON DC//N2/N6F1133//, COMSPAWARSYSCOM SAN DIEGO CA//PMW161//, SPAWARSYSCEN ATLANTIC CHARLESTON SC//80P/526CS/721SR//, CMIO NORFOLK VA//N3//, the applicable COR, CONAUTHs of all required COMSEC material, and local ~~CMS Advice and Assistance~~ COR Audit Team. AMD-9

(b) **Marine Corps Commands**:

Submit to NCMS WASHINGTON DC//N31//, CMC C FOUR CY WASHINGTON DC//, info COMMARCORSYSCOM QUANTICO VA//CINS//, administrative Chain of Command, COMSPAWARSYSCOM SAN DIEGO CA//PMW161//, SPAWARSYSCEN ATLANTIC CHARLESTON SC//80P/526CS/721SR//, CNO WASHINGTON DC//N2/N6F1133//,CMIO NORFOLK VA//N3//, the applicable COR, CONAUTHs of all required COMSEC material, and local ~~CMS Advice and Assistance~~ COR Audit Team. AMD-9

(c) **Coast Guard Commands**:

Submit to NCMS WASHINGTON DC//N31//, COGARD C4ITSC ALEXANDRIA VA//BOD-IAB//, INFO COMLANTAREA COGARD or COMPACAREA COGARD, administrative Chain of Command, SPAWARSYSCEN ATLANTIC CHARLESTON SC//80P/526CS/721SR//, COMSPAWARSYSCOM SAN DIEGO CA//PMW161//, CNO WASHINGTON DC//N2/N6F1133//, CMIO NORFOLK VA//N3//, the applicable COR, CONAUTHs of all required COMSEC material, and local ~~CMS Advice and Assistance~~ COR Audit Team. AMD-9

(d) **Naval Reserve Commands**:

Submit to NCMS WASHINGTON DC//N31//, COMNAVRESFOR//01A2//, info administrative Chain of Command, SPAWARSYSCEN ATLANTIC CHARLESTON SC//80P/526CS/721SR//, COMSPAWARSYSCOM SAN DIEGO CA//PMW161//, CMIO NORFOLK VA//N3//, CNO WASHINGTON DC//N2/N6F1133//, the applicable COR, CONAUTHs of all required COMSEC material, and local ~~CMS Advice and Assistance~~ COR Audit Team. AMD-9

f. **Identification of Required Material**:

All COMSEC material (e.g., keying material, equipment and related devices, cryptographic system operating instructions (KAOs) and maintenance manuals (KAMs), etc.) must be specifically identified by short title and desired quantity.

g. **NCMS Action**:

NCMS will establish an EKMS account based on the information contained in the request, assign an EKMS account number, which also serves as the EKMS ID.

h. **Actions required to ensure receipt of COMSEC material (after an establishment request has been approved)**:

(1) The EKMS Manager must coordinate with the area Defense Courier Service (DCS) station and establish a DCS account by submitting a USTRANSCOM Form 10. DCS Manual 5200.1 (series) contains the administrative and operational procedures of the DCS. Consistent with granting access and signature requirements for a CMS Form 1, and ~~IMT~~Form-10 ~~forms~~ will be signed by the **current** Commanding Officer, SCMSRO, or OIC, as applicable or other official "Acting" in such capacity. AMD-9

NOTE: Commands must ensure that NCMS//N31// and CMIO//N3// are informed of their DCS address upon initial establishment of courier service and whenever there is a change in their DCS address.

(2) EKMS account commands that expect to draw equipment over-the-counter (OTC) from CMIO must submit a CMS Form 1 listing EKMS personnel to CMIO in order to receipt for and courier COMSEC equipment for their command. Annex H contains a sample and instructions for completing a CMS Form 1.

(3) Upon receipt of an account establishment message reflecting the account number assigned to the command from NCMS, the command must establish a User Representative (UR) account with the EKMS Central Facility (CF). This is accomplished through completion and submission of a CF Form 1206 to the commands Command Authority (CA). The requesting command must complete sections D and E; the CA is responsible for completion of sections B, C, and G of the form. The CA will submit the completed and signed form to the CF via either fax or as an attachment to a digitally signed email. If a CA has not been assigned or is unknown, submit the completed form to NCMS Attn: Key Division. Action will not be taken on any request submitted

via email which is not digitally signed.

(4) The account/command must also establish a Department, Agency, Organization (DAO) code. This is accomplished through completion and submission of a CF Form 1202 to either the CA or NCMS Key Division as discussed above. The requesting command must complete section D; the CA will complete sections B, C, and F. If multiple DAO codes are to be established, a CF Form 1203 is also required. A CF Form 1207 must be completed and submitted to order material for the respective DAO and if multiple DAOs are registered a CF Form 1208 (User Representative DAO Privilege Registration Request Continuation) must also be completed and submitted to the CA or NCMS, as applicable.

Note: All forms mentioned herein, including instructions for completing each can be found at: www.iad.nsa.gov/keysupport

(5) When an installation date for the LMD/KP is received, the command not the installation team must submit a request for a FIREFLY Vector Set (FF), Message Signature Key (MSK), and (2) KSV-21 cards with EKMS privileges in accordance with Article 670 to this manual. NCMS will only order KSV-21 cards to be used with the LMD/KP. All other KSV-21 cards must be ordered by the EKMS Manager/Alternate for the unit requiring such. If the aforementioned keys are not received and held NLT 14 days prior to the scheduled installation, contact NCMS Key Division for assistance.

(6) Within seven working days of installation of the LMD/KP, commands are required to submit a message to NCMS//N3// to certify their completion of all requirements for Navy EKMS accreditation. A sample message can be found in Annex AA.

410. SELECTION OF EKMS PERSONNEL (GENERAL REQUIREMENTS):

Individuals selected must:

a. Be responsible and qualified to assume the designated COMSEC duties for the respective position appointed to or designated for.

b. Be in a position or level of authority to permit them to exercise proper jurisdiction in fulfilling their responsibilities.

c. Be a permanent government employee (Civilian government employee or Military). Contractors may **not** be appointed to EKMS positions except as indicated in articles 414 and 416 below.

d. Be a U.S. citizen, includes naturalized. Resident aliens are **not** eligible and may **not** have access to material classified above the CONFIDENTIAL level.

e. Not have been previously relieved of COMSEC duties for reasons of poor performance.

f. Not be assigned collateral duties which will interfere with their duties. When appointing EKMS personnel, the Commanding Officer must consider the size of the account, the number of LEs supported, the location where the LEs operate, and Two-Person Integrity (TPI) requirements.

g. (**For EKMS Managers, LE Issuing and Alternates**) not be temporarily assigned to the command on Temporary Additional Duty (TAD) orders, but be permanently assigned to or employed by the command, as applicable dependent upon status (civilian government employee or military member).

h. Be authorized access to COMSEC material, in writing by the current Commanding Officer.

i. Review and execute a SD Form 572.

Note: Electronic signatures are acceptable on SD Form 572s, provided all legal requirements (e.g., authenticity, non-repudiation, verification, and records management/storage) are met. Legal requirements include, but are not limited to, Article 15 U.S.C. 7001, 7006 and 7021. DOD CAC or NSS PKI Tokens meet these requirements.

j. Complete required training, including applicable portions of NAVEDTRA 43462 (EKMS PQS) for the position to which appointed or designated (EKMS Manager, Alternate EKMS Manager, LE Issuing, LE Using(EKMS User), EKMS Clerk, etc... Applicability for completion and exemptions to PQS requirements are outlined in article 312.

412. DESIGNATION REQUIREMENTS FOR EKMS MANAGERS AND ALTERNATES:

In addition to the criteria set forth in articles 410 and 505, the following are required for appointment as either an EKMS Manager or Alternate EKMS Manager.

a. **Minimum Personnel**:

1. Each numbered account will have an EKMS Manager, and a minimum of one alternate appointed by the current Commanding Officer. The use of "By Direction" is **not** authorized for Letters of Appointment or for granting access to COMSEC material.

2. For accounts with an HCI of TS, an additional two alternates is **highly** recommended to have at least two personnel who have either the "A" or "B" combinations, as applicable for TPI purposes during periods of leave, TAD, etc…

3. Individual appointment letters will be updated when new or additional personnel are assigned and upon change of command.

NOTE: When there is a change of command, existing appointment letters must be updated/signed by the CO/OIC within 60 days of assumption of command.

b. **Grade and Length of Service Requirements (EKMS Managers)**:

1. **Navy Accounts:** EKMS Managers must meet the following minimum grade requirements: Enlisted E6 (or selectee), GS7/Pay Band 1, or a Commissioned Officer.

2. **USCG, USMC and MSC Accounts:** Enlisted E6 (or selectee), GS-7/Pay Band 1 or Commissioned Officer.

3. Regardless of service affiliation, both civilian government employees and Commissioned Officer's appointed **must** have a minimum of six months government/commissioned service, as applicable which does not include duty under instruction or in training but may include six or more years of prior enlisted service for Commissioned Officers.

4. For civilian government employees to be appointed as EKMS Managers or Alternates, the position description must specify EKMS Manager duties as a full-time position, prior to appointment as EKMS Manager.

c. **Grade and Length of Service Requirements (Alternate EKMS Managers)**:

1. Alternate EKMS Managers must at a minimum be an Enlisted E5, GS6/Pay Band 1, or a Commissioned Officer.

2. Both civilian government employees and Commissioned Officer's appointed must have a minimum of six months government/commissioned service, as applicable which does not include duty under instruction or in training but may include six or more years of prior enlisted service for Commissioned Officers.

3. If **none** of the designation requirements were previously waived, fully qualified and appointed personnel who have performed the duties of an EKMS Manager or Alternate EKMS Manager within the past 12 months may be re-appointed.

4. For civilian government employees to be appointed as EKMS Managers or Alternates, the position description must specify the EKMS Manager duties as a full-time position, prior to appointment as EKMS Manager.

d. **Security and Access Requirements**:

1. EKMS Managers and Alternates must possess a security clearance equal to or higher than the Highest Classification Indicator (HCI) of the account.

2. If the account is validated for/holds keying material intended for use on SCI/SI circuits, both the EKMS Manager and Alternates **must be** SCI eligible and indoctrinated at the time of appointment.

3. If the eligibility has been established and is reflected in JPAS but the indoctrination cannot be conducted at the time of appointment, the command may request a waiver from NCMS to afford the time for doing so. If granted, the account must ensure the physical destruction at the account level of keying material used to protect SCI/SI information is conducted adhering to strict Two Person Integrity (TPI) procedures with a minimum of one of the two personnel being SCI indoctrinated. **This will not be waived and is required by National policy.**

4. Temporary access (interim clearance) may be granted by the Commanding Officers per the guidance outlined in Art 9-4 to SECNAV M5510.30 however; temporary access for SCI may only be authorized by DON CAF.

5. EKMS Managers and Alternates must be authorized

access to COMSEC material, in writing by the current Commanding Officer.

6. EKMS Managers and Alternates must execute and have on file a SD Form 572 found in Annex K.

e. **Length of Appointment**:

There is no restriction on the length of time an individual may be appointed as an EKMS Manager or Alternate EKMS Manager.

f. **Training Requirements for EKMS Managers and Alternates**:

1. **Navy/Coast Guard Accounts:** Personnel selected to be an EKMS Manager or Primary Alternate EKMS Manager must successfully complete the Navy EKMS Manager's Course of Instruction (COI) (V-4C-0013) **prior to** appointment.

AMD-9

a. When training cannot be completed prior to appointment due to quota non-availability, operational requirements, etc… personnel appointed must complete the EKMS Manager Job Qualification Requirement (JQR) which is available from the servicing ~~CMS AA training~~ COR Audit team.

b. EKMS Managers completing the above mentioned JQR pending the completion of formal training must complete the Navy EKMS COI within 90 days of appointment. Alternate EKMS Managers must complete the course within 180 days of initial appointment.

2. **USMC Accounts:** Personnel selected to be the EKMS Manager or Primary Alternate EKMS Manager must successfully complete the EKMS Manager's Course of Instruction (COI) (V-4C-0013) within 180 days of appointment. Pending completion of formal training, personnel may be appointed as Tertiary Alternates and receive On-The-Job-Training and perform required duties under instruction.

3. EKMS Managers or Alternates unable to attend formal training within the 90 or 180 day time frame specified above **require** a waiver from NCMS to continue performing duties as the EKMS Manager or Alternate, as applicable beyond the periods specified.

4. Personnel Qualification Standards (PQS) Completion.

(a) As outlined in Article 312.

414. DESIGNATION REQUIREMENTS FOR LOCAL ELEMENT (LE) ISSUING PERSONNEL AND EKMS CLERKS:

In addition to the general requirements set forth in articles 410 and 505 to this manual, EKMS personnel appointed as a LE (Issuing or Using), EKMS Clerk or EKMS Witness must also meet the requirements set forth in this article.

a. **Minimum Personnel**:

Commanding Officers of units where an LE (Issuing) is appointed must also appoint a minimum of one Alternate LE (Issuing). Alternate LEs Issuing are equally responsible with the Primary LE Issuing for the proper management of COMSEC material and oversight to LE personnel. The appointment of additional alternates beyond the minimum of one is at the **discretion** of the Commanding Officer. The use of "By Direction" is not authorized for Letters of Appointment or granting access to COMSEC material.

For LE Issuing that require material classified at the TS level, an additional two alternates is **highly** recommended to have at least two personnel who have either the "A" or "B" combinations, as applicable for TPI purposes during periods of leave, TAD, etc…

Individual appointment letters will signed by the current Commanding Officer and updated upon change of command.

NOTE: When there is a change of command, existing appointment letters must be updated/signed by the CO/OIC within 60 days of assumption of command.

b. **Grade and Length of Service Requirements For LE (Issuing):**

1. **LE Issuing (for keying material designated as CRYPTO)**: Personnel appointed must be U.S. Government employees either meeting the following minimum grade requirements: military (E-5) or civilian (GS5/Pay Band 1).

2. **LE *Issuing*** (**for CCI and/or keying material *not* designated CRYPTO)** may be either U.S. Government employees (military or civilian employee, E5, GS5, or Pay Band 1), as applicable or contractors.

~~c. **Training Requirements For LE Issuing and Alternates:**~~

AMD-9

~~1. Primary LE (Issuing) and their Alternate(s) must complete the CMS Local Element Interactive Courseware within 30 days after appointment.~~

~~2. LE commands will ensure that course completion is documented and that a copy of the completion certificate is entered into the LE's service record.~~

AMD-9

~~3. A copy of the completion certificate must be forwarded to the EKMS Manager of the supporting account and retained with the Appointment Letter for the respective LE (Issuing).~~

c~~d~~. **Security and Access Requirements**:

1. For LEs (Issuing or Using) personnel must have a security clearance equal to or higher than the highest classification of material issued to/or held by the LE.

2. For LEs (Issuing and Using) including Alternates, SCI indoctrination is only required **if material intended for use on SCI/SI circuits is issued to/used by the LE**.

3. LE personnel must be authorized access to COMSEC material, in writing by the current Commanding Officer.

4. LE personnel must execute and have on file a SD Form 572.

416. DESIGNATION REQUIREMENTS FOR LOCAL ELEMENT (LE) USING AND EKMS WITNESSES:

a. In addition to the general requirements set forth in articles 410 and 505, the following apply to both LE Using and EKMS Witnesses.

1. Personnel appointed to serve as LEs ***Using***, EKMS Clerks, or EKMS Witnesses may be U.S. Government employees or contractors.

2. Personnel selected must be either a natural born or naturalized U.S. citizen.

3. Possess a security clearance equal to or higher than the highest classification of the COMSEC material being handled.

4. Be responsible individuals and qualified to execute

his/her assigned COMSEC duties.

b. **Additional Training Requirements For LE Issuing, Alternates, LE Using and EKMS Clerks:**

1. Complete applicable portions of the latest EKMS PQS (NAVEDTRA 43462 series) as outlined in Article 312. There is no PQS for a witness.

418. APPOINTMENT LETTER/MEMORANDUM:

a. EKMS Managers, Alternates, Clerks and LEs (Issuing) must be formally designated in an individual Appointment Letter or Memorandum signed by the current Commanding Officer. The use of "By Direction" is **not** authorized for appointment letters or granting access to COMSEC material.

b. Letters or Memorandums of Appointment will be maintained locally at the command in accordance with Annex T.

c. LEs (Issuing) must forward a copy of the letter/memorandum to the parent or servicing EKMS account.

d. Letters of appointment must contain, at a minimum all information reflected in the sample found in Annex J.

e. Letters of appointment are not to be submitted to NCMS.

NOTE: When there is a change of command, existing appointment letters must be updated/signed by the CO/OIC within 60 days of assumption of command.

420. WAIVERS:

a. Commanding Officers are authorized to waive the length of government service required for EKMS Managers. Waivers of this requirement must be documented **locally** and retained by the account and the unit's ISIC until no longer in effect. Do **not** submit copies of these waivers to NCMS.

b. Waivers of all other requirements must be submitted as follows:

Type Command:	**Action Addressee**:
Navy (subordinate to Combatant	COMUSFLTFORCOM

Commander)	COMPACFLT
Marine Corps	CMC C FOUR CY WASHINGTON DC//
MSC	COMSC//N62//
Coast Guard	COGARD C4ITSC//BOD-IAB//
Naval Reserve	COMNAVRESFOR//01D//
Navy (not subordinate to a Combatant Commander)	NCMS//N5//

c. If approved, waivers will be granted for the minimum duration required for the unit to comply with the policy in which the waiver was obtained for and up to a maximum of one year. Waivers are **not** automatically renewed by NCMS and should a valid operational requirement exist which necessitates the need for the waiver beyond one year, the requesting activity is responsible for resubmitting the waiver request prior to the expiration of the existing waiver.

422. MANAGEMENT OF MORE THAN ONE ACCOUNT BY AN EKMS MANAGER AND ALTERNATE

a. COs or OICs will not designate the currently appointed EKMS Manager and Alternate to serve simultaneously as managers of more than one EKMS account except in instances where the command also has an approved special mission account.

b. In such instances, prior to appointment, authorization must be obtained from NCMS//N5//.

c. If authorized by NCMS, COs/OICs may appoint a single EKMS Manager and Primary Alternate to serve under the command's multiple accounts.

423. TEMPORARY ASSUMPTION OF DUTIES AS AN EKMS MANAGER:

a. The EKMS Manager may not be absent for more than 60 days.

b. During the temporary absence of the EKMS Manager, the Primary Alternate EKMS Manager must administer the account but may not do so for longer than 60 days.

c. Any absence of the EKMS Manager for longer than 60 days requires the appointment of a new EKMS Manager.

d. The Commanding Officer of the account command may authorize an account inventory before, during, or after the temporary absence of the EKMS Manager.

425. GRANTING OF TEMPORARY ACCESS

a. In accordance with the CNO policy ltr 5510 Ser N09N2/7U223012 dated 26 Jan 07, Commanding Officers or Officers in Charge may grant temporary access to individuals pending completion of full investigative requirements and pending establishment of security clearance eligibility by the DON CAF.

b. When necessary to minimize operational impact, commands granting Temporary Access must strictly adhere to the provisions set forth in the latest CNO guidance and must record clearance data, including temporary access in JPAS/JCAVS to ensure the Personnel Security Investigation (PSI) is opened in a timely manner. Such data must be available during audits.

c. Temporary access or assignment to sensitive positions is NOT authorized for individuals who have received an unfavorable eligibility determination.

d. Questionable or unfavorable information that becomes available related to individuals granted access to classified material will be handled in accordance with SECNAV M5510.30 (series) Article 9.7.

e. Temporary access for SCI requires authorization from DON CAF **prior to** granting access.

f. USCG EKMS Managers must consult COMDINST M5520.12 (series) in the granting of interim clearances.

430. HIGHEST CLASSIFICATION INDICATOR (HCI):

a. The Highest Classification Indicator (HCI) is used to determine the highest classification of COMSEC material that an account may hold. The HCI is determined by the requesting authority based on need. Once the HCI is set, all personnel managing the account must be cleared to the HCI of the account.

> **NOTE: Carefully consider both short and long-term needs when determining the HCI for an account. Once an account's LMD/KP is initialized with a given HCI, it cannot be easily changed. Changing a HCI necessitates the initialization of the LMD/KP with the "new" HCI and re-entry of all COMSEC material holdings into LCMS. Additionally, initialization of the LMD/KP with the "new"**

HCI results in the loss of "all" electronic key held under the "old" HCI, regardless of classification.

b. NCMS establishes the account at the level requested and maintains the HCI records for DON EKMS accounts and provides this information to the National Security Agency (NSA).

c. The HCI is checked by the NSA, CMIO, and USNDA prior to shipping COMSEC material to an account. COMSEC material is released for shipment only after it has been determined that the HCI equals or exceeds the classification of COMSEC material to be shipped.

d. HCI information must be included in a request to establish an EKMS account. Thereafter, commands must submit a letter or message to NCMS//N3// if they want to change the HCI.

435. CHANGE OF COMMAND TITLE/ADDRESS/CLAIMANCY SHIFT:

a. **Common Account Data (CAD)**. Commands that undergo a shift in claimancy or a name change will refer to EKMS 704 (series) for instructions on modifying their own Common Account Data (CAD)and uploading account registration changes and credentials to the Directory Server. This information will then be used to update the COR database. For name and/or address changes, you will also need to update your DCS two-line address by submitting new USTRANSCOM Form 10(s) to your servicing DCS station. The importance of maintaining the accuracy of this information cannot be overemphasized. It is the responsibility of individual commands to keep this information as current as possible. Failure to do so can and has resulted in missed/severely delayed COMSEC material shipments and in Loss of Control COMSEC material incidents.

440. EKMS RESPONSIBILITIES:

a. **Immediate Superior in Command (ISIC)**. ISICs are responsible for the EKMS accounts of their subordinate commands by:

(1) Validating the operational requirement for an EKMS account.

(2) Determining COMSEC material allowance requirements and, when required, obtaining CONAUTH authorization in accordance with Article 405.c.

(3) Ensuring that physical security inspections are conducted.

AMD-9

(4) ~~Conducting EKMS account inspections and forwarding copies of reports of inspection findings to NCMS//(N7)//.~~ If not deferred to CMS COR Audit Teams, will conduct CMS COR Audits of subordinate accounts.

(5) Reviewing and/or retaining COMSEC records pending receipt of NCMS notice of reconciliation upon account disestablishment.

b. **Staff CMS Responsibility Officer (SCMSRO)**:

AMD-9

(1) A flag or general officer in command status, or the Deputy Commander or Chief of Staff, may either assume personal responsibility for routine COMSEC matters or may designate , in writing, a SCMSRO. SCMSROs must have a security clearance equal to or higher than the highest classification of COMSEC material held by the account and be senior to EKMS manager (0-4(**or selectee**)/GS-12/Pay Band 2 or above).

(2) A designated SCMSRO is responsible for the proper administration of routine matters for an EKMS account but may also exist at a LE organization as stated in Article 135.

(3) SCMSROs must sign COMSEC correspondence and reports as "Staff CMS Responsibility Officer" vice "By direction."

(4) Duties of the SCMSRO cannot be further delegated and must revert to the appointing official in the absence of the assigned SCMSRO.

(5) Specific duties are identical to Commanding Officer duties and responsibilities listed in Article 450.

NOTE: Assignment of a SCMSRO does not relieve the appointing official of ultimate responsibility for the proper management of an EKMS account. The SCMSRO may delegate two of the CO spot checks to the Communications Officer (COMMO), as long as the COMMO is not designated as the EKMS Manager or Alternate.

c. **Chain of Command**:

(1) The management and security of COMSEC material are inherent responsibilities of all levels of command. Proper

evaluation of COMSEC administrative procedures can be made only if all officers in the Chain of Command are knowledgeable and support compliance with established COMSEC procedures and requirements.

(2) In performing routine administrative duties, the EKMS Manager will normally report to the Communications Officer for functional direction and administration. However, the EKMS Manager must have direct access to the Commanding Officer for Operational COMSEC needs.

d. **EKMS Manager**:

(1) The individual designated in writing by the current Commanding Officer who is responsible for all actions associated with the receipt, handling, issue, safeguarding, accounting, and disposition of COMSEC material assigned to an EKMS account.

(2) He/she is responsible to the Commanding Officer for the performance of his/her COMSEC duties and will normally report to the Commanding Officer for operational COMSEC needs and the Communications Officer for routine (administrative) duties requiring functional direction and administration.

(3) He/she shares the responsibility with the Commanding Officer/Officer in Charge for ensuring that all EKMS Alternate(s) are properly trained in accordance with the requirements of this manual.

e. **Alternate EKMS Manager(s)**:

(1) The individual(s) designated in writing by the current Commanding Officer who is/are responsible for assisting the EKMS Manager in the performance of COMSEC duties and for assuming the duties of the EKMS Manager in his/her absence.

(2) Alternate EKMS Manager(s) report to the EKMS Manager for COMSEC duties and share equally with the EKMS Manager the responsibility for the proper management and administration of an EKMS account.

f. **Local Element(s)**:

(1) LE personnel are designated in writing by the current Commanding Officer and are responsible for the proper handling and accounting of the COMSEC material received from the parent or servicing EKMS account (or from LE (Issuing)

personnel).

(2) LEs, irrespective of command relationships, must adhere to the procedures in this publication and written instructions issued by the EKMS Manager.

(3) All LE personnel must execute a SD Form 572 as shown in Annex K.

g. **EKMS Clerk (formerly referred to as "Account Clerk")**:

(1) EKMS Clerks are designated in writing by the current Commanding Officer and are responsible for assisting EKMS personnel in the execution of administrative duties associated with the management of an EKMS account.

(2) Assignment of an EKMS Clerk is at the **discretion** of the Commanding Officer.

h. **EKMS Witness**:

(1) An EKMS Witness is responsible for assisting EKMS personnel in the proper execution of routine administrative tasks related to the handling and safeguarding of COMSEC material (e.g., receipt, destruction, inventory, or maintaining TPI).

(2) An EKMS Witness must be familiar with applicable procedures of this manual and all command-issued directives governing the handling of COMSEC material with respect to the task being performed.

(3) An EKMS Witness must be authorized access, in writing, to keying material.

(4) Assignment of an EKMS witness is at discretion of commanding officer.

NOTE: An EKMS Clerk may function as an EKMS Witness but an EKMS witness may not necessarily be an Account Clerk.

445. LETTER OF AGREEMENT (LOA):

a. In those instances where a LE is responsible to a Commanding Officer other than that of the numbered EKMS account command or issuing activity, a Letter of Agreement (LOA) must be executed between the EKMS account command and the LE command.

NOTE: Throughout this manual, the terms "Letter of Agreement", "Memorandum of Agreement" and "Memorandum of Understanding" are used interchangeably.

b. Annex L contains a sample Letter of Agreement with the minimum requirements to be addressed.

c. Letters of Agreement remain in effect until modified or the support is no longer required. LOAs/MOUs will be reviewed at a minimum of triennially.

d. Inventory requirements for LEs supporting through a Letter of Agreement (LOA) are outlined in Articles 766.a.3.d and 766.a.4 (note).

450. RESPONSIBILITIES AND DUTIES: COMMANDING OFFICER

Commanding Officers are ultimately responsible for the proper management and security of all COMSEC material held by his/her command and must:

a. Ensure compliance with established policy and procedures governing the safeguarding and handling of COMSEC material.

NOTE: Throughout this manual, responsibilities/duties applicable to Commanding Officers apply equally to Staff CMS Responsibility Officers (SCMSROs) and Officers-in-Charge (OICs), unless otherwise indicated. These responsibilities and/or duties also apply equally to the Commanding Officers and OICs of LEs.

b. Appoint in writing qualified and responsible individuals as EKMS Manager and Alternate Manager(s), Local Elements (Issuing), and, if desired a EKMS Clerk.

c. Establish in writing a list of personnel authorized access to keying material.

d. Ensure that training procedures are adequate to meet operational requirements.

e. Ensure that COMSEC incident reports are promptly submitted and action taken as required.

f. Extend cryptoperiods as applicable. Commanding

Officers (cryptonet members) can extend cryptoperiods for two hours without Controlling Authority authorization when necessary to complete a transmission or conversation. There is no reporting requirement for this type of extension. The Controlling Authority must approve longer cryptoperiod extensions.

g. Ensure that the EKMS PQS (NAVEDTRA 43462 series) is incorporated into the command training program in accordance with Article 312.

NOTE: EKMS PQS does not apply to MSC/USCG/USMC personnel.

h. Ensure that local procedures are established for identification and reporting of any potentially significant changes in life-style, financial status, or disciplinary problems involving personnel authorized access to COMSEC material; and that those changes are reported to the Command Security Manager and if appropriate, the Special Security Officer (SSO).

i. Ensure that spot checks are conducted at least quarterly, of the COMSEC Vault and spaces where COMSEC material is used and stored. The CO may delegate **no more than two** of the four quarterly inspections to the Executive Officer (XO). The SCMSRO may delegate **no more than two** to the Communications Officer (COMMO) as long as the COMMO is not designated as the EKMS Manager or Alternate. See below notes for additional guidance on Spot Checks.

NOTE: (1) LE (Issuing or Using) Commanding Officers/OICs, including those in locations remote from the servicing or parent EKMS account, are responsible for conducting quarterly spot checks in accordance with Article 465 of this manual. Servicing/parent EKMS accounts may require the reporting of spot check results; such a requirement should be spelled out in the LOA/MOU between the servicing command and the command being serviced.

(2) Additional spot checks by other senior, properly cleared chain of command personnel, i.e. Commo, Operations Officer, Executive Officer, etc… are highly encouraged but at the discretion of the CO, ISIC or TYCOM.

(3) EKMS Managers and/or Alternates will conduct a minimum of one spot check per month (minimum 12 per calendar year).

(4) The size of the account and number of LEs supported must be considered to determine if the minimum number of spot checks (16 per account) is adequate to ensure the proper management of the account and security of COMSEC material. Doing the minimum 16 per account(4 by the CO and 12 by the Manager) would not serve as a true indicator of the health of the account when the number of LEs is greater than the minimum spot checks required. It is highly recommended that spot checks not be repeatedly conducted on the same LEs to maximize oversight and training. Follow-up spot checks should be conducted and training provided when discrepancies are noted.

AMD-9

j. Receive debriefings from ~~CMS Advice and Assistance (A&A) Training Teams and~~ CMS COR ~~Inspectors~~ Auditors.

k. Ensure that comments on personnel performance of Managers are included in fitness reports, enlisted evaluations, and civilian performance appraisals, as applicable.

l. Ensure that manager assignments are documented in an individual's service record or position description, as applicable.

m. Ensure that the Emergency Action Plan (EAP)/Emergency Destruction Plan (EDP) is established and tested. Annex M contains guidance for developing an EAP.

NOTE: Commands located outside the U.S. and its territories and deployable units must also have and exercise at a minimum of annually an Emergency Destruction Plans (EDPs).

n. Ensure that an inventory of all COMSEC material held by an account is conducted in conjunction with a change of Commanding Officer as required by Article 766, upon change of EKMS Manager, and semiannually as required.

o. Ensure the EKMS Manager position is a primary duty.

p. Active involvement by Commanding Officer/SCMSRO in oversight of EKMS Manager operations has shown to be single common factor in preventing major insecurities.

q. For external LEs supported through a LOA/MOA/MOU, an inventory is required when a Change of Command or Change of LE

Issuing, as applicable occurs as discussed in Articles 766.a.3.d and 766.a.4(note) herein.

NOTES: 1. CO responsibilities onboard MSC ships will be performed by the Ship's Master except for T-AGOS (SURTASS) ships where they will be performed by the embarked mission supervisor.

2. CO responsibilities on board T-AH (hospital) ships will be performed by the ship's master when the ship is in a full operational status (FOS) and by the Officer-in-Charge of the assigned Medical Treatment Facility (MTF) when the ship is in a reduced operational status (ROS).

3. A CO whose command includes remote detachments may choose to allow a remote detachment to establish its own independent EKMS account. If the title of the separate EKMS account states "Detachment" or the equivalent, the responsible authority in charge of the unit is automatically authorized to sign routine COMSEC documents which would otherwise require the signature of the CO(e.g., accounting inventory or destruction records). The delegation of other command COMSEC responsibilities is at the discretion of the CO, who may wish to have such a COMSEC intra-command relationship formally recorded. A formal record or description of duties delegated is optional and should not be forwarded to NCMS.

455. RESPONSIBILITIES AND DUTIES: EKMS MANAGER

EKMS Managers are responsible for all actions associated with the receipt, handling, issue, safeguarding, accounting, and disposition of COMSEC material assigned to an EKMS account and also serves as the Commanding Officer's primary advisor on EKMS account management matters. In this capacity, the EKMS Manager must:

a. Provide the Commanding Officer and other interested personnel with information about new or revised COMSEC policies and procedures and their impact on the command.

b. Acquire, monitor, and maintain the command COMSEC material allowance. This includes an annual review of all COMSEC material holdings to ensure that there is a continuing need for the quantity and types of all COMSEC material held. Material held in excess of operational requirements should be identified by submitting a routine modification to an allowance in accordance with Chapter 6.

c. Maintain proper storage and adequate physical security for the COMSEC material held by the account.

d. Keep Alternate Manager(s) informed of the status of the account so that the Alternate(s) are, at ALL times, fully capable of assuming the duties of the EKMS Manager.

e. Provide LE(s) written guidance or appropriate extracts from this publication as well as any other manuals and instructions (see Article 721) necessary for the accurate and secure handling/accounting of COMSEC materials.

f. Conduct training, at a minimum of monthly to ensure that all personnel handling COMSEC material are familiar with and adhere to proper COMSEC procedures. Training for operation of fill device applications and interfaces to end-use items is the responsibility of the program manager of record. Information on how to get training on fill device applications is available through the SPAWAR EKMS Help Desk. Document training locally in accordance with command directives and retain in accordance with Annex T. EKMS Managers are also responsible for the proper training of remote LEs and for ensuring that the Commanding Officers/OICs of their remote LEs (Issuing) are conducting quarterly spot checks as required (Article 465 pertains). EKMS Managers are encouraged to require their remote LE Commanding Officers/OICs to report spot check results; such a requirement should be spelled out in the LOA/MOU between the servicing or parent account and the command being serviced.

> **NOTE:** Training can be accomplished via a variety of methods including but not limited to; facilitated training, required reading, distribution and reviewing of presentations, during spot checks with LE personnel, etc… **regardless of medium used what is important it is that training is; (a) ongoing, (b) accomplished, (c) documented and (d) verifiable.**

g. Maintain records and files as required by this manual.

h. Ensure prompt and accurate preparation, signature, and submission of account correspondence, message, and accounting reports.

i. Issue COMSEC material on local custody form(s) after verifying that the recipient is authorized to hold COMSEC material and has executed a SD Form 572 ~~COMSEC Responsibility Acknowledgment Form~~. AMD-9

j. Load electronic key from LCMS to fill device for end user requirements. Operation of fill device application to end item is responsibility of operator with end item training.

k. Oversee the implementation of and compliance with Over-the-Air-Rekey (OTAR)/Over-the-Air-Transfer (OTAT) procedures (e.g., periodic review of local logs, adherence to TPI requirements).

l. Ensure that LEs properly inventory and destroy COMSEC material issued to them through periodic documented spot checks.

m. Ensure that procedures are established to reassign local custody responsibility for COMSEC material held by individuals permanently leaving the command, and those who are departing on TAD/TDY in excess of 30 days.

n. Ensure that all amendments to this manual and other COMSEC-related publications are entered promptly and correctly.

o. Maintain the account's portion of the command Emergency Action Plan (EAP) and/or Emergency Destruction Plan (EDP). Annex M contains guidance for developing an EAP/EDP.

NOTE: Commands located outside the United States, its territories and deployable units must have both an EAP and EDP.

p. Conduct required inventories and destruction of COMSEC material in accordance with this manual.

q. Ensure proper physical security measures are maintained when COMSEC material is transported within the command.

r. Ensure that COMSEC material is properly packaged and shipped via an authorized method as required by this manual.

s. Ensure page checks of COMSEC material are conducted as required.

t. Ensure that TPI requirements are adhered to in accordance with this manual.

u. Ensure that modifications to COMSEC equipment are promptly and properly performed by qualified individuals in accordance with OPNAVINST 2221.3 (series) and that modification residue is disposed of properly.

v. Report immediately to the CO any known or suspected PDS or COMSEC Incident in accordance with this manual and initiate action to ensure that required reports are submitted and replacement material is, when required, obtained.

AMD-9

w. Advise the CO when more than 24 months have passed since the last ~~ISIC-conducted EKMS inspection~~ COR Audit. An audit ~~formal inspection~~ is required every 24 months in accordance with Article 315.b.

x. Verify the security clearances of all personnel prior to granting them access to/issuing them COMSEC material.

y. Perform a Semi-annual Self-Assessment of the account using EKMS-3 (series).

z. Ensure a Local Element Spot Check is performed as discussed in Article 450.i (NOTE 3).

aa. Perform required LCMS backups.

ab. Perform a KP changeover as described in Article 238.

ac. Perform KP rekeys annually or more frequently, as required.

ad. Maintain Common Account Data (CAD) and upload changes to account registration and credentials to the Directory Server.

ae. Ensure monthly or more frequent Audit Trail reviews are conducted on storage devices possessing audit capability. See Annex Z paragraph 17.c(note 3) and Annex AF paragraph 9.b note 3) for exemptions to the Audit Trail review policy.

af. Ensure adequate personnel are authorized to order Modern Key from the EKMS Central Facility and submit updated CF forms as necessary. See Annex AE for additional guidance.

ag. Track and manage production and destruction dates for Modern Key held by the account and ensure timely submission of key orders for replacement material required NLT 30 days from the expiration date of the keys currently held as discussed in

Article 670.

ah. Ensure the EKMS Manager Turnover Checklist is conducted in accordance with Annex Y.

460. RESPONSIBILITIES AND DUTIES: ALTERNATE MANAGER

a. Alternate Manager(s) have the same duties and responsibilities as the EKMS Manager and are equally responsible to the Commanding Officer for the proper management and security of all COMSEC material held by the command.

b. On a continuing basis, Alternate Manager(s) must be actively involved in the daily operation of the account and; be ready at all times to fully administer the account in the absence of the EKMS Manager.

465. RESPONSIBILITIES AND DUTIES: LOCAL ELEMENT

NOTE: The responsibilities of Local Element (LE) Commanding Officers/OICs are outlined in Article 450. COs/OICs/SCMSROs of external commands are required to conduct a minimum of (1) spot check per quarter within their organization where COMSEC material is used/stored. The LOA/MOU between the supporting and the supported commands may outline additional requirements.

Local Element (LE) personnel are responsible to their Commanding Officer for the proper management and security of all COMSEC material held by the command. LEs are responsible to the parent or servicing account (or to the LE (Issuing)) for the proper accountability, security, control, and disposition of COMSEC material issued to them. LEs must also:

a. Provide the Commanding Officer of the LE command with information about new or revised COMSEC policies and procedures and their impact on the command.

b. Follow written instructions issued by the parent or servicing EKMS account (or LE (Issuing)) governing the handling, accountability, and disposition of COMSEC material.

c. Provide written guidance concerning handling, accountability, and disposition of COMSEC material to all LE (Using) personnel. Conduct training to ensure that all personnel handling COMSEC material are familiar with and adhere to proper COMSEC procedures. Emphasis shall be placed on accountability, security, TPI requirements, and identification of improper practices. Fill device applications and end unit interface training is responsibility of program of record. Document training locally in accordance with command directives.

d. Ensure proper inventory and destruction of COMSEC material issued to the LE (Using) personnel.

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

f. Ensure that all amendments to COMSEC-related publications are entered promptly and correctly, as applicable.

g. Complete, maintain, and forward required accounting records and reports to the parent or servicing EKMS account (or LE (Issuing)).

h. Issue COMSEC material on local custody forms after verifying that the recipient is authorized to hold COMSEC material and has executed a ~~Responsibility Acknowledgment~~ SD Form 572. AMD-9

i. Oversee the implementation of and compliance with the OTAR/OTAT procedures (e.g., periodic review of local logs, adherence to TPI requirements).

j. Ensure that page checks of COMSEC material are conducted as required.

k. Ensure adherence to TPI requirements.

l. Incorporate emergency destruction procedures for COMSEC material into the LE command Emergency Action Plan (EAP). Refer to Annex M for guidance on an EAP.

m. Report immediately to the LE Commanding Officer and the parent or servicing account EKMS Manager (or LE (Issuing)) any known or suspected Practices Dangerous to Security (PDS), or COMSEC Incident in accordance with this manual. Coordinate with the parent or servicing EKMS account (or LE (Issuing)) to ensure that required reports are submitted and replacement material is, when required, obtained.

n. All LE personnel must execute a SD Form 572 as shown in Annex K.

470. **RESPONSIBILITIES AND DUTIES**: **EKMS CLERK**

a. EKMS Clerks, if assigned, must; be designated in writing by the current Commanding Officer and receive training from the EKMS Manager in the physical security and administrative responsibilities associated with COMSEC material.

b. EKMS Clerks perform the following:

(1) Execute routine administrative duties and assist EKMS personnel with general file maintenance.

(2) Maintain TPI requirements after security containers containing Top Secret keying material marked CRYPTO have been opened by EKMS personnel.

(3) Assist in conducting page checks and entering amendments and corrections into COMSEC and COMSEC-related publications.

(4) Sign receipt, inventory, and destruction reports, as an EKMS **witness only**.

(5) Assist in the placement of status markings on COMSEC material.

(6) Accompany/assist EKMS personnel in maintaining TPI when picking up COMSEC material from a CMIO, USNDA or courier, and during the processing and/or transfer of COMSEC material.

c. **Restrictions**: EKMS Clerks **ARE NOT** authorized to:

(1) Have knowledge of/or access to the combinations of security containers storing COMSEC keying material.

(2) Destroy, receive, transfer or inventory COMSEC material other than in the presence of EKMS Manager personnel.

(3) Be registered as an operator/administrator or authorized to perform functions on the LMD/KP.

480. **RESPONSIBILITIES AND DUTIES**: **EKMS WITNESS**

An EKMS Witness, if assigned, is required to be familiar with the applicable procedures of this manual and related command-issued directives. An individual who witnesses an inventory, destruction, or any other COMSEC report is **equally** responsible for:

a. Accuracy of the information listed and the validity of the report or record used to document the transaction being witnessed.

b. Sighting all material inventoried when signing an inventory report.

c. Sighting all material to be destroyed and witnessing the actual destruction of the material.

d. Adhering to TPI requirements.

CHAPTER 5 -- SAFEGUARDING COMSEC MATERIAL AND FACILITIES

FIGURES:

CHAPTER 5 - SAFEGUARDING COMSEC MATERIAL AND FACILITIES

501. GENERAL:

a. The ultimate effectiveness of protections provided to COMSEC material, systems and equipment are dependent upon the actions of each individual COMSEC user.

b. The security achieved through the proper use of cryptosystems is to a large extent dependent upon the physical protection afforded the associated keying material and those facilities where this material is stored.

c. Each person authorized access to COMSEC material as a user or witness, when required is personally responsible for:

(1) The proper safeguarding, accountability, usage and disposal of the material.

(2) Promptly reporting to proper authorities any occurrence, circumstance, or act which could jeopardize the security of COMSEC material.

d. This chapter prescribes the minimum security requirements.

e. Construction specifications for shore-based COMSEC storage vaults used to store keying material which were designed and approved prior to 01 Jan 2013 are contained in Annex N.

f. Construction specifications for shore-based COMSEC storage vaults used to store keying material constructed or modified after 01 Jan 2013 will be in accordance with ICD-705.

g. COMSEC facilities that hold only manual cryptosystems, unclassified keying material for machine cryptosystems, or publications other than full maintenance manuals are exempt from the facility construction requirements of this manual.

505. ACCESS AND RELEASE REQUIREMENTS FOR COMSEC MATERIAL:

a. **Security clearance**: Access to classified COMSEC material requires a security clearance equal to or higher than the classification of the material. LMD/KP System Administrators and Operators must be formally trained and possess a security clearance equal to or higher than the HCI of the account. With exception to accounts validated for keying material used to protect SCI/SI information, appointment can be based on an interim security clearance. See Chapter 4 for details. Access to unclassified COMSEC material **does <u>not</u>** require a security clearance. Revocation of a security clearance revokes access.

b. **<u>Requirement for Access or Need-to-Know</u>**: Access to classified and unclassified COMSEC material must be <u>restricted</u> to properly cleared individuals with a valid need-to-know whose <u>official</u> duties require access to COMSEC material. The fact that an individual has a security clearance, and/or holds a certain rank or position, does <u>not</u> in itself entitle an individual access to COMSEC material.

c. **<u>Briefing/Indoctrination</u>**: All individuals granted access to COMSEC material must be properly indoctrinated regarding the sensitivity of the material, the rules for safeguarding such material, the procedures for reporting COMSEC incidents, the laws pertaining to espionage (Title 18, U.S.C., Sections 793, 794, and 798), and the rules pertaining to foreign contacts, visits, and travel. See SECNAV M5510.30 (series) for the minimum security education requirements for DON commands.

d. **<u>Written Access to COMSEC Keying Material</u>**: All personnel having access to cryptographic information (keying material, book packaged material marked/designated crypto, or equipment which permits extraction of key (DTD, SKL, TKL, LMD/KP) **<u>must</u>** be authorized <u>in writing</u> by the current Commanding Officer or "Acting Commanding Officer". The use of "By Direction" is **not authorized** in granting access to COMSEC material. An individual designation or appointment letter may be used for this authorization or such may be reflected on an access list to the space in which the individuals are assigned.

(1) Individual letters remains in effect until the status of the individual changes (i.e., a change in clearance status, transfer, separation, retirement of assignment to duties no longer requiring access.

(2) Access lists when used for granting access to COMSEC cryptographic information will be updated whenever the status of an individual changes, upon Change of Command or annually, at a minimum.

e. **<u>Personnel Access</u>**:

(1) <u>U.S. Citizens</u>: U.S. citizens including naturalized who

are U.S. Government employees, DOD contractors, military personnel, including Naval Reserve personnel performing active duty training or assigned to drill units may be granted access to COMSEC material if they are properly cleared, their duties require access, and applicable briefings are executed.

(2) Resident Aliens: Resident aliens and foreign nationals who are employed as U.S. Government civilian or military personnel, who have been lawfully admitted into the U.S. may have access to unclassified COMSEC material, if their duties require such access. While only U.S. citizens are eligible for a security clearance, a resident alien or foreign national may be granted a "Limited Access Authorization" (LAA) in compliance with DoD 5200.2-R section C3.4.3. Such individuals may have access to COMSEC material **no higher** than CONFIDENTIAL, if they have an LAA based on a completed successful background investigation and indoctrination, on a "need to know" basis, when their duties require such access.

(a) Resident aliens **may not** be appointed as EKMS Managers, Clerks, or equipment maintenance personnel nor have access to safes or areas where COMSEC keying material is accounted for, visible, or stored.

(3) Foreign nationals will not be granted access to, or provided information about, COMSEC keying material without written permission from the material's Controlling Authority. Access to other COMSEC material must be approved by NSA//DP22//.

(4) Security Guard Personnel:

(a) Guards whose official duties require access to COMSEC material must meet the access requirements of this chapter and be instructed concerning their responsibilities. Except in emergency situations, unescorted access to the LMD/KP is prohibited.

(b) Guards who are not given access to COMSEC material and who are used to supplement existing physical security measures need not meet the access requirements of this chapter.

(5) Industrial Personnel:

The Commanding Officer may authorize industrial personnel (e.g., naval shipyard personnel) access to classified communications spaces when required. Applicable guidance related to access to devices and or specific cryptosystems can be found in the Cryptographic Operating Manual (KAO) or Operational Security Doctrine (OSD) for the device. Classified material not marked or designated as crypto, will be protected in accordance with SECNAV M5530.36 (series).

f. **Contractor Personnel**:

U.S. Government COMSEC operations are normally conducted by U.S. Government personnel. However, when there is a valid need and it is clearly in the best interest of the DON and the U.S. Government, COMSEC equipment, keying material (including manual COMSEC systems), related COMSEC information, and access to classified U.S. Government information may be provided to properly cleared, U.S. contractor personnel when block 10 to the DD-254 (contract) stipulates the access is required to:

(1) Install, maintain, or operate COMSEC equipment for the U.S. Government.

(2) Participate in the design, planning, production, training, installation, maintenance, operation, logistical support, integration, modification, testing or study of COMSEC material or techniques.

(3) Electronically communicate classified national security information in a cryptographically secure manner or unclassified national security-related information by COMSEC protected means.

g. **Release of COMSEC Material to a Contractor Account**:

1. The release of COMSEC material to a contractor account or direct issuance to contractor personnel as LEs by a DON COMSEC account is restricted to U.S. Industrial firms operating under contract to the U.S. Navy in accordance with the provisions of OPNAVINST 2221.5 (series). All requests for release of material to a contractor account or direct issuance to contractor personnel requires prior approval from NCMS. The request must be submitted by the Contracting Office Representative (COR), and will not be accepted from the project officer or EKMS Manager. Requests must include the following:

(a) Identity of Navy project office/contracting office

(b) Contractor name, COMSEC Account Number (if none so state) and address

(c) Contract number

(d) Contractor facility clearance and location where the functions will be performed

(e) Nature and scope of the contractual functions

(f) The COMSEC Material or cryptographic equipment to which the contractor/contractor account will have access

(g) The number of contractor personnel involved

(h) The initial date contractor personnel will have access to COMSEC material or equipment and the length of the contract or period of time such access will be required

(i) Expiration date of the contract

(j) Any other information deemed appropriate in evaluating the request

2. The Contracting Office must supply either a copy of the DD-254 or certify in writing that block 10a of the DD-254 was checked as requiring access to COMSEC Material.

3. In the event that the requirements of OPNAVINST 2221.5 (series) were not fulfilled prior to release of COMSEC material to a contractor/contractor account, permission after-the-fact must be obtained from NCMS//N3// by submitting the following information:

a. Identity of Navy project office/contracting office

b. Contract number and expiration date

c. List of COMSEC material/cryptographic equipment provided to the contractor and date provided

d. Contractor facility clearance and location

e. Name and contact information for the contractor/contractor account number

NOTE: The return of COMSEC equipment for repair/return to a vendor such as VIASAT, General Dynamics, etc., will be documented using local custody procedures.

h. **Access to COMSEC Equipment (less CCI)**:

(1) Keyed: Access to keyed COMSEC equipment, including CHVP is restricted to personnel possessing holding a security clearance equal to or higher than the classification of the equipment or keying material, whichever is higher whose official duties require access. Access by resident aliens is restricted to the CONFIDENTIAL level as stated in Article 505 above.

(2) Unkeyed: Access to unkeyed COMSEC equipment may be granted to U.S. citizens whose official duties require access and who possess a security clearance equal to or higher than the classification of the equipment.

NOTE: Access requirements for CCI can be found in Article 535.

i. **Displaying, Viewing, and Publicly Releasing COMSEC Material and Information**:

(1) Open public display of U.S. government or foreign government COMSEC material and information at non-governmental symposia, meetings, open houses, or for other non-official purposes is **prohibited**.

(a) This includes discussion, publication, or presentation for other than official purposes.

(b) No external viewing or other exposure which might afford opportunity for tampering or internal examination is permitted.

(2) Photographs, drawings, or descriptive information for press release or private use is prohibited.

(3) Exterior photographs of COMSEC equipment used for command training need not be marked “FOR OFFICIAL USE ONLY” and existing FOUO markings may be removed or obscured.

(4) Refer requests for public or non-official display or publication of COMSEC material and information, and Freedom of Information Act (FOIA) requests to: COMNAVIDFOR SUFFOLK VA //N6//info DIRNSA//S5/I01P//.

(5) All contracts involving COMSEC information or material shall contain a binding non-disclosure statement to prevent the publishing of COMSEC-related information without prior approval

of the contracting office.

j. **Release of COMSEC Material to a Foreign Government**:

Requests by foreign governments or international organizations for COMSEC material or requests to release COMSEC material to foreign governments resulting from DON operational commitments, shall be processed as follows:

(1) Submit requests with supporting data and recommendations via the chain of command to:

(a) Your command's Navy Component Commander (as listed in the Standard Navy Distribution List) if subordinate to a COMFLT or FMF Commander; **OR**

AMD-9

(b) CNO WASHINGTON DC//N6F// or CMC C FOUR CY WASHINGTON DC~~//C4/C4 CY/C4 IA~~// if not subordinate to a COMFLT or FMF Commander.

(2) Provide copies of all such requests to the Navy International Program Office, Washington, D.C., and to DIRNSA FT GEORGE G MEADE MD//DP22//.

k. **Ship Rider Procedures**: Occasionally a valid operational requirement may exist in which U.S. military personnel embark on an allied vessel for coalition and/or combined operations such as; PASEX, RIMPAC, etc… When such will involve the installation, handling, storage and use of COMSEC material, in addition to the procedures contained in this manual, EKMS Managers must review and adhere to the procedures outlined in CJCSI 6510.06(series) which can be found at www.js.smil.mil/masterfile/sjsimd/jel/cdata/limited/6510_06.pdf

510. TWO-PERSON INTEGRITY (TPI) REQUIREMENTS:

a. **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.

(1) TPI handling requires that at least two persons, authorized access to COMSEC keying material, be in constant view of each other and the COMSEC material requiring TPI whenever the material is accessed and handled.

(2) TPI storage requires the use of an approved COMSEC vault or GSA approved security container. Vault doors or GSA approved security containers must have the required GSA approved label on the outside. With exception to field safes, vault doors and GSA approved security containers will be equipped with a FF-L-2740/2740A or higher locking mechanism programmed with (2) different combinations to prevent a single person from having access.

b. **Material Requiring TPI at the EKMS Manager Level**:

TPI must be applied to the following COMSEC material from time of receipt through the time of destruction, issue or transfer, as applicable for the following:

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

(2) Fill Devices (FDs) or other physical media (removable media such as floppy disks, magnetic tapes, etc.) storing unencrypted TOP SECRET key.

(3) Equipment containing TOP SECRET key that allows for key extraction.

c. **TPI Handling and Storage Requirements at the EKMS Manager Level**:

(1) Access to and knowledge of combinations protecting material subject to TPI at the Manager level must be restricted to only the EKMS Manager and Alternate(s). No one Manager will have access to or knowledge of both "A" and "B" combinations to any one TPI container/safe.

(2) All TOP SECRET COMSEC material evolutions (e.g., destruction, generation, issue (physical or to a DTD, SKL, TKL, etc…, importing, possession, receipt or transfer) conducted at the Manager level must always be conducted by the EKMS Manager and Alternate, the Manager or an Alternate and a properly cleared person.

(3) After a container holding material subject to TPI at the Manager level has been opened by the authorized combination holder(s) (i.e., EKMS Manager and Alternate(s)), any properly cleared person who has been granted access to the material (e.g., account clerk) may assist the EKMS Manager or Alternate in maintaining TPI and with locking the container and/or the vault.

(4) TPI is required when receipting for material from DCS and the account's HCI is TOP SECRET or when transporting TOP SECRET COMSEC material to DCS or to/from another account. LE personnel with a clearance (within scope) equal to or higher than the HCI with of the account are authorized to accompany the Manager or Alternate in the delivery or pickup of COMSEC material subject to TPI. Provided the package is not opened and remains sealed to prevent access, other properly cleared and authorized personnel who accompany the Manager or Alternate are not required to be SCI eligible. Such personnel will not be used to open, inspect and receipt for the contents if they are not authorized access to COMSEC material in writing and SCI eligible and indoctrinated (if the account is validated for keying material used to protect SCI/SI information). The two individuals receipting for the material are responsible for maintaining TPI until the material is locked in a TPI approved container.

(5) When material requiring TPI is not being handled, it must be locked in a TPI-approved security container as specified in Article 520.

(6) TPI is required when a TS Administrator or Operator CIK is created on a Key Processor (KP) where the HCI is TS.

d. **TPI Handling and Storage at the Local Element Level**:

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:

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

(2) 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.

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

(4) Unloaded FDs in an operational communications environment containing keyed crypto-equipment which permits extraction of unencrypted TOP SECRET key.

NOTE: TPI is not required if the equipment does not permit extraction of key or the equipment key ports are protected against unauthorized key extraction using a TPI-approved locking device/physical barrier. In this case the unloaded FDs may be stored under single lock protection.

(5) 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.

Note: When not in use, material requiring TPI must be protected by a TPI-approved locking device/physical barrier (in the case of equipment) or locked in a TPI storage container as specified in Article 520.

KGX-93/KG-83 NOTES:

1. **Single-person access to the unrestricted commands is authorized. Restricted commands must be accessed in accordance with TPI rules and when not manually accessed, restricted commands must be protected by the specially designed locking bar.**
2. **When not in use, the "Dutch Doors" allowing access to a KG-83 must be properly secured with TPI locking devices.**

e. **TPI for Keyed COMSEC Equipment**:

(1) TPI is required when unencrypted TOP SECRET keying material marked or designated CRYPTO is inserted into and extracted from COMSEC equipment and when loaded into FDs.

(2) The following methods are authorized to maintain TPI on keyed COMSEC equipment from which classified key marked or designated CRYPTO can be extracted:

(a) The continuous presence of at least two authorized persons, in sight of each other and the keyed equipment.

(b) Use of a metal cage or steel mesh divider secured with two approved locks.

(c) Installation of two approved locks on access doors to spaces where keyed COMSEC equipment is located. **Cipher locks are not acceptable for this purpose; cipher locks are for personnel access control only.**

(d) Installation of fabricated metal bars to the equipment racks, secured with two approved locks. The bars should traverse the card reader covers in such a manner that the bars must be removed in order to gain access to the keying material. Do not attach the bars to the equipment itself because the alteration will constitute an unauthorized modification.

(e) Installation of a video monitoring or surveillance system in such a manner that the monitoring screen and the equipment or material can be viewed constantly.

(f) Assign additional personnel so that spaces are manned by a minimum of two properly cleared and authorized persons who are in view of each other and the material at all times.

f. **TPI Exceptions:**

(1) 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.

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

NOTE: Loaded FDs placed in an Air Crew comm box locked with TPI approved combination locks fulfills TPI requirements. One air crewmember may transport the locked comm box up to the flight line boundary. Loaded FDs may be stored onboard the aircraft in a single-lock container while the aircraft is in a flight status.

(3) Crypto Repair Facilities (CRFs), maintenance facilities, and laboratory environments are not required to maintain TPI for FDs where operational key is not handled.

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

(5) In facilities/spaces used solely for the storage of unkeyed equipment.

(6) Flag (e.g., COMFLT) communicators operationally deployed away from their primary headquarters are exempt from TPI requirements.

(7) Unless required by TYCOM, ISIC or local policy, TPI is **not required** for COMSEC keying material marked SECRET or below regardless of CRYPTO markings.

(8) KG-83 or KGX-93 key variable generators when the "Dutch Doors" are properly secured with TPI locking devices.

g. **Requirement to Report TPI Violations**:

Any loss of TPI required by this manual must be reported in accordance with Article 945.

515. ACCESS TO AND PROTECTION OF SAFE COMBINATIONS, KP PINs AND (SCO) PASSWORDS

a. **Selection of Combinations**:

Each lock must have a combination composed of randomly selected numbers based on constraints of the manufacturer. The combination must not deliberately duplicate a combination selected for another lock within the command and must not be composed of successive, systematic or predictable sequences of numbers (e.g., birth dates, social security numbers, and phone numbers).

b. **Requirements for Changing a Combination**:

Combinations must be changed as follows:

(1) When the lock is initially placed in use. A manufacturer preset combination **may not** be used.

(2) When any person having knowledge of the combination no longer requires access (e.g., loss of clearance, transfer) unless other sufficient controls exist to prevent access to the lock.

(3) When the possibility exists that the combination has been subjected to compromise (e.g., a container opened by unauthorized personnel in an emergency situation).

(4) When the lock has been taken out of service.

(5) When any repair work has been performed on the combination lock.

(6) At least once every two years or sooner as dictated by the above events.

c. **Access and Knowledge of Combinations**:

Only properly cleared and authorized individuals will have knowledge of and access to combinations protecting COMSEC material. Access and knowledge of these combinations will be restricted as follows:

(1) Personnel Authorized to Change Manager Vault/Safe Combinations: Only cleared individuals who have been formally authorized access to keying material by the Commanding Officer shall change combinations.

(2) Manager Vault/Safe Combinations: Except in an emergency, the combinations to the EKMS Manager's Vault and/or safe(s) will be known only by the EKMS Manager and Alternate(s). **No one individual will have access to or knowledge of the "A" and "B" combinations to any one TPI safe/container.**

(3) Combinations to TPI Containers: No one person may change both combinations used to maintain TPI. Neither will the same authorized individual try or verify (for the purpose of preventing a lockout) both newly changed combinations to a TPI container. A certified locksmith may be used to prepare locks for new combinations, but the actual combination must be selected and entered by an individual authorized access to that combination.

> **NOTE: In the case of a single Alternate only, each newly changed TPI combination shall be tried or tested only by the Manager or Alternate authorized knowledge of or access to a particular combination. Specifically, only the Manager or Alternate authorized access to or knowledge of combination "A" may try or test combination "A"; the same restriction applies to the "B" combination.**

(4) Requirement to Report Unauthorized Access or Knowledge of Combinations to TPI Containers: Except in an emergency, if one person gains knowledge of both combinations, change both combinations, inventory the material, and report the matter as a Physical Incident in accordance with Chapter 9.

d. **Classification of Combinations**: Lock combinations shall be classified and safeguarded based on the highest classification of material protected by the combination.

e. **Records of Combinations**: To provide for emergency access, a central record of the lock combinations for all COMSEC material security containers must be maintained in another GSA-approved security container (**other than the container where COMSEC material is stored**) approved for storage based on the highest classification of material protected by the combination locks.

f. **Sealing/Wrapping Combinations, KP PINs and LCMS (SCO) passwords**: Combinations to COMSEC material security containers, KP PINs and LCMS passwords must be protected as follows:

(1) Combinations, KP PINs and LCMS passwords must be recorded and individually wrapped in aluminum foil and protectively packaged in a separate SF-700 combination envelope.

(2) SF-700s used to record the password/PIN of an individual (single person) LMD/KP Administrator or Operator may be recorded on a single SF-700. Although LCMS passwords are considered SECRET, if the HCI of the account is TS, and the individual in which the password/pin pertains is privileged at the TS level, both Part 2 and 2A of the associated SF-700 will be classified, stored and safeguarded at the TS level. Passwords or PINS for different personnel will not be stored on SF-700s used to record PINS and/or passwords for other registered users.

(3) SF-700s will be sealed with lamination paper, plastic tape or commercially available tamper-indicating envelopes to easily identify tampering or unauthorized access during monthly inspections as discussed below.

(4) The name(s) and addresses of the individual(s) authorized access to the combinations must be recorded on the front of the envelope. Current DoD policy considers personal addresses and telephone numbers Personally Identifiable

Information (PII) and requires that Part 1 of SF-700s used for combinations be sealed in an opaque envelope prior to posting inside the door or container, as applicable. If unsealed, Part 1 must be resealed no later than the following working day.

NOTE: For personnel who reside onboard a ship annotate the berthing compartment/stateroom location and rack number on the SF-700 vice the generic term "onboard."

(5) Individual protectively wrapped envelopes may be stored in the same single-lock security container.

NOTE: Combinations protectively packaged in accordance with the preceding guidance do not require TPI handling/storage.

(6) For further guidance on KP PINs and LCMS passwords see Article 520.

(7) SF-700s must be inspected monthly to ensure they have not been tampered with. Monthly SF-700 inspections will be documented utilizing a locally generated spreadsheet/inventory log. At a minimum, the following must be recorded: the date of inspection and both the printed name and signature of the individual conducting the inspection.

g. **Emergency Access to Containers and Combinations**:

In an emergency, the Commanding Officer or other designated authority may direct the opening of any COMSEC material security container.

(1) At least **two** individuals shall be present to conduct and witness the emergency opening.

(2) After an emergency opening, the official who opened the container will make an after-the-fact report to the person in charge of the container.

(3) The individual(s) responsible for a container opened in an emergency must immediately conduct a complete inventory of the COMSEC material, and change the combinations as soon as possible.

h. **Personal Retention of Combinations**:

It is specifically **prohibited** for an individual to record, carry or store insecurely for personal convenience, combinations to COMSEC facilities, security containers or PINS and/or passwords in electronic form in a computer, calculator, or similar electronic device.

i. **Adjustment of pre-configured default password parameters on LMD (LCMS SCO Password Lockout and/or Reset):**

(1) The LMD is pre-configured to lock out accounts after 3 failed attempts and also to request a password change every 90 days. These system settings were designed to maximize LMD/KP system security and should be verified by EKMS Managers upon receipt of a new hard drive or assumption of duties. If discovered to be set at a greater interval, the EKMS Manager or Alternate will modify the password change frequency to 90 days to ensure compliance with the systems Certification and Accreditation (C&A) documentation.

(2) Personnel authorized access to the LMD/KP are further authorized to make temporary changes to the pre-configured default password parameters for the purpose of restoring a lockout or setting up new Administrators. Upon completion of the task, the default password parameter must be reset to three.

(3) If unauthorized adjustments or suspicious activity is detected on the LMD, consult local, service-specific Information Assurance or SECNAVINST 5239.3 (series) guidance for any required reporting.

(4) The reporting of the above as a COMSEC incident is only required if, based on a review of Article 945 an incident may have or is known to have occurred.

520. STORAGE REQUIREMENTS:

a. **General**:

(1) The LMD/KP including connecting cables, must be maintained, operated, and stored in a space approved for the open storage of SECRET material. If not approved for open storage at the SECRET level, the LMD's hard drive and KP must be removed and stored in a GSA approved security container approved for SECRET or higher storage when the space is not occupied. Access to the area, space, or container must be limited to individuals with a minimum clearance of SECRET.

(2) Store COMSEC material only in containers and spaces approved for their storage. **Unless COMSEC material is under the**

direct control of authorized persons, keep the containers and spaces locked.

(3) Comply with applicable information on supplementary controls (e.g., guards and alarms) for safeguarding classified material in accordance with SECNAV M5510.36 (series).

(4) 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, Aides) and classification (T.S., Secret, Confidential, Unclas). 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.

(5) COMSEC keying material designated for NATO use may be stored with other COMSEC material.

(6) Unless absolutely necessary, do **not** place COMSEC material containers in commonly used passageways or other spaces where access cannot be controlled. During non-working hours, security containers should be located in locked areas and not accessible to general traffic.

(7) COMSEC keying material in electronic form stored in the LMD is considered "UNCLASSIFIED CRYPTO" because it is encrypted.

(8) Annex N contains construction specifications for storage vaults.

b. **Required Forms for Storage Containers**: Storage containers for COMSEC material require the following forms:

(1) **SF-700:** Part (1) of a classified container information form (Standard Form 700) for each lock combination must be placed on the inside of each COMSEC storage container. Current DoD policy considers personal addresses and telephone numbers to be PII and requires Part 1 be sealed in an opaque envelope prior to posting inside the container or door, as applicable. Part 1 is not classified; Parts 2 and 2A will be classified based on the classification of the highest content in the container and

must reflect the following derivative and downgrading instructions: "Derived from: 32 CFR 2001.80(d)(3)" "Declassify: Upon Change of Combination".

(2) **SF-702:** A security container open/closure log (Standard Form 702) must be maintained for each lock on a COMSEC storage container. Each opening and closure of the container must be annotated on the accompanying Standard Form 702. A separate SF 702 will be used for each FF-L-2740/2740A combination. **Completed SF-702s will be retained in accordance with Annex T.**

(3) **OF-89:** A Maintenance Record for Security Containers and Vault Doors (Optional Form 89) must be prepared and maintained for each container/lock/vault door, as applicable when put in use and is intended to serve as a permanent record and retained for the service life of the security container or vault door. All repairs to damaged security containers must conform to Federal Standard 809 titled Neutralization and Repair of GSA-approved containers and Vault Doors. 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.

c. **Storage of COMSEC Keying Material Marked or Designated CRYPTO**:

Classified COMSEC keying material marked or designated CRYPTO must be stored as indicated below:

(1) Storage at Shore Stations:

(a) Store TOP SECRET keying material in a strongbox or special access control container within a vault **or** in a GSA approved security container equipped with a locking mechanism meeting FF-L-2740/FF-L-2740A requirements.

(b) Store SECRET keying material in a COMSEC vault **or** in any security container approved for storing SECRET or TOP SECRET keying material.

(c) Store CONFIDENTIAL keying material in a file cabinet having a built-in three-position manipulation-resistant dial-type combination lock, **or** in any storage container approved for storing SECRET **or** TOP SECRET keying material.

(d) Unclassified DES COMSEC keying material marked or designated CRYPTO must be stored in the most secure manner available to the user (i.e., approved safes, if available, locked file cabinets, key-locked rooms, containers, etc.)

(2) Storage Onboard DON Ships:

(a) Store TOP SECRET keying material in a GSA approved security container with an electro-mechanical lock meeting Federal Specification FF-L-2740/FF-L-2740A, **or** in a strong room, **or** in any storage container approved for storing TOP SECRET keying material at shore stations.

(b) Store SECRET keying material in a steel security filing cabinet having a lock bar secured with three position, changeable combination padlock meeting Federal Specification FF-P-110J or an electro-mechanical lock meeting Federal Specification FF-L-2740/FF-L-2740A procured from GSA, in a strong room, in any storage container approved for storing SECRET or TOP SECRET keying material at shore stations.

(c) Store CONFIDENTIAL keying material in a file cabinet secured with an electro-mechanical lock meeting Federal Specification FF-L-2740/2740A, in any storage container approved for storing SECRET or TOP SECRET keying material at shore stations.

(d) Unclassified DES COMSEC keying material marked or designated CRYPTO must be stored in the most secure manner available to the user (i.e., approved safes, if available, locked file cabinets, key-locked rooms, containers, etc.).

(3) Storage in Tactical Situations: TOP SECRET and below keying material may be stored in a standard, approved field safe **or** similar security container secured by an electro-mechanical lock meeting Federal Specification FF-L-2937, FF-L-2740, or FF-L-2740A standards or a high security combination lock meeting Federal Specification FF-P-110J requirements.

(4) Residential Security Containers: Must be secured to the building structure.

d. **Two-Person Integrity Storage Containers**:

(1) COMSEC material requiring TPI storage at the Manager level may be stored using any one of the following options:

(a) Inside a COMSEC Vault equipped with one manufacturer built-in combination lock on the door, and the TPI material stored in a GSA approved container equipped with a FF-L-2740/2740A lock.

(b) Inside a COMSEC Vault, where the vault door is equipped with a combination lock that meets FF-L-2740/2740A specifications programmed with (2) different combinations.

(c) In a GSA approved security container with combination lock meeting FF-L-2740/2740A specifications programmed with (2) different combinations.

REMINDER: Combinations to the account's COMSEC vault or GSA approved security containers at the account level are restricted to the EKMS Manager and Alternates only.

(2) COMSEC material requiring TPI storage at the LE level must be stored under one of the following options:

(a) Inside a COMSEC Vault equipped with one manufacturer built-in combination lock on the door, and the TPI material stored in a GSA approved container with a FF-L-2740/2740A.

(b) Inside a COMSEC Vault where the vault door is equipped with a combination lock that meets FF-L-2740/2740A specifications programmed with (2) different combinations.

(c) In a GSA approved security container with combination lock meeting FF-L-2740/2740A programmed with (2) different combinations.

(d) In a special access control container (SACC) securely welded to the interior of a GSA approved security container drawer.

e. **Restriction on Use of Modified GSA Approved Security Containers and Vault Doors**:

(1) **NO** external modifications are authorized for GSA approved security containers and vault doors after 14 April 1993.

NOTE: *Modification* is defined as any change to the overall configuration of the safe/vault's original design. For example, replacing a malfunctioning combination lock (a one-for-one swap out/replacement) on a vault door or a security container does *not* constitute a modification. Boring a hole through a vault door or security container, on

the other hand, does constitute a modification.

(2) If external modifications are made, the GSA approved security container label and the material must be removed from the container. The container or vault door is no longer authorized for protecting **any** classified material.

(3) GSA security containers and vault doors externally modified for TPI requirements prior to 14 April 1993 may continue to be used.

(4) The available options for storing TPI material in a GSA container or vault externally modified prior to 14 April 1993 is as follows:

(a) Store COMSEC material requiring TPI in a separate safe within the COMSEC Vault or in a Special Access Control (SACC) that has been fastened (welded to the interior of one of the drawers of the CMS safe).

(b) Install a combination lock meeting FF-L-2740/2740A specifications programmed with (2) different combinations on the door to the COMSEC vault. The following may be used in place of two built-in combination locks:

1 An approved combination padlock meeting FF-P-110 (e.g., Sargent and Greenleaf (S&G) model 8077A/8077AB). A hardened steel hasp will be electrically welded to the door of the vault.

2 A steel mesh divider, with an approved combination padlock meeting FF-P-110J installed within the COMSEC Vault.

3 Install two combination locks or use an approved combination padlock meeting FF-P-110J with a hardened steel hasp electrically welded to the COMSEC safe(s) located outside the COMSEC Vault.

4 Install two approved locks on security containers used to store or hold COMSEC material requiring TPI in the LE Issuing/User spaces.

f. **Locking Devices**:

The following locking devices are approved for satisfying TPI requirements on equipment:

(1) S&G combination padlock, model 8077A/8077AB.

(2) Standard Navy issue brass key padlocks.

(a) Each lock must be individually keyed and master keys to a series of locks are not permitted.

(b) All keys used to control access to COMSEC equipment must be strictly controlled as turn-over items on a watch-to-watch inventory. Keys cannot be removed from the spaces.

g. **Storage and Protection of COMSEC Equipment**

Access to the LMD/KP is restricted to properly cleared and authorized personnel only. The LMD must be disconnected when the associated STE is used for NON-EKMS purposes. Remote dial-in access from another site is prohibited.

(1) Some COMSEC equipment may, based on its configuration, require special storage facilities and procedures that are normally addressed in the handling section of the operational security doctrine for the system.

(2) In conjunction with any special requirements, the following guidance must be used to store and protect COMSEC equipment:

(a) Store unkeyed equipment based on the classification of the equipment (if classified) and in a manner sufficient to preclude any reasonable chance of pilferage, theft, sabotage, tampering, or access by unauthorized persons. See Article 535 for storage requirements for unkeyed CCI.

NOTE: When installed in an operational configuration (e.g., in a ship, aircraft, shelter, vehicle, backpack or building) classified unkeyed COMSEC equipment may be left unattended, provided the Commanding Officer or other responsible Authority judges it is protected sufficiently to preclude any reasonable chance of pilferage, theft, sabotage, tampering, or access by unauthorized persons.

(b) Protect all keyed equipment, including Cryptographic High Value Products (CHVP) based on the classification of the equipment or the keying material, whichever is higher. Additionally, ensure that procedures are in effect to prevent unauthorized use of the equipment or extraction of its key.

(c) When equipment containing encrypted key is located in an unmanned space, the CIK must be removed and protected in another location.

(d) Keyed DES equipment and key loaders will be controlled and protected in the most secure manner available to the user.

(e) Unkeyed DES equipment and key loaders will be controlled and protected as high value property and will not be released to foreign nationals without prior approval from NSA (DP22).

(3) Protect computer systems performing COMSEC functions by hardware and software controls to prevent unauthorized access and penetration. Protect machine readable copies of COMSEC programs in accordance with their classification.

h. **Storage of Fill Devices (FDs)**:

(1) At either the account or LE level, FDs loaded with unencrypted TOP SECRET key marked or designated CRYPTO must be provided TPI storage.

(2) At the LE level, TPI storage must be provided for unloaded FDs in an operational communications environment which contains keyed equipment from which unencrypted TOP SECRET key marked or designated CRYPTO may be extracted. This includes DTDs, SKLs, etc… when the CIK is inserted, accessible or not secured in a TPI approved container.

(3) TPI storage is not required for modern storage devices which make use of CIKS to permit or prohibit access to protected unencrypted TOP SECRET key such as DTDs, SKLs, TKLs, etc… when the associated CIK is removed and stored separately in a GSA-approved container in accordance with Annex Z, AF or the Operational Security Doctrine for the device, as applicable.

i. **Storage of Other COMSEC Material**:

(1) KP CIKs such as Transit CIKs, Administrator CIKs, or Operator CIKs are classified SECRET based on the classification of LMD and KP. CIKS are not categorized as crypto and will be stored in a GSA approved security container when not in use. A single LMD/KP operator may generate TOP SECRET key on the LMD/KP

however, two personnel are required to "output" the generated key in red form. Because CIKS cannot be used without knowledge of the associated PIN and LCMS records all functions perform by the administrator or operator, CIKS are not subject to TPI handling or storage.

(2) REINIT 1 and NAVREINIT 2. REINIT 1 and NAVREINIT 2 KSD-64As are classified at the level of the HCI of the account; are not designated crypto; are not subject to TPI handling or storage; are **NOT** "KP CIKS"; are not used to generate or output key; and are only used when necessary to reinitialize a replacement KP. **New REINIT 1 and NAVREINIT 2s are created when an account loads a new Message Signature Key (MSK). New NAVREINIT 2s are created when a changeover is conducted as discussed in Article 238 and Annex X.**

REINIT 1 is assigned AL Code 1 and registered with the material type "***COMSEC Aide***" in LCMS. NAVREINIT 2 is assigned AL Code 4 and registered with the material type "***Equipment***" in LCMS. For additional information related to accountability of REINIT 1 and NAVREINIT 2s, see Article 1185.

(3) KP Operational EKMS FIREFLY Key: The FIREFLY vector set is; classified based on the HCI of the account; designated as CRYPTO; accounted for based on an assigned ALC of either 1 or 6 and permits the ability to generate and exchange necessary credentials to transfer or receive keying material up to the HCI. FF Vector Sets will be stored and safeguarded in accordance with this chapter.

(4) KP Operational EKMS Message Signature Keys (MSK): The MSK is; classified based on the HCI of the account; designated as CRYPTO; accountable as either ALC-1 or 6 and shall be stored and handled accordingly as specified in this chapter.

(5) Consistent with the classification of the LMD, all magnetic media, including backup media, floppy diskettes, etc… used in the LMD/KP must be classified and safeguarded at the SECRET level. Printed matter will be classified, based on the content which may only be UNCLAS/FOUO.

(6) KP CIK PINS will be safeguarded at the level the manager or alternate is privileged at minimum SECRET however, if the HCI of the account is TOP SECRET, the PINS should be TOP SECRET as well as the KP requires (2) appropriately privileged personnel to output TOP SECRET key.

(7) LCMS passwords are classified and will be protected stored and safeguarded at the SECRET level, unless an individual records his/her password and PIN on a single SF-700 and the individuals PIN is privileged at the TOP SECRET level. When so done, the SF-700 will be properly labeled and safeguarded at the TOP SECRET level.

(8) PINS, like passwords will not be written down on any document other than a SF-700. Each manager or alternate will have their own SF-700 for their PIN/password. PINS must be changed at a minimum of every 90 days or upon a change of personnel.

(9) SF-700s used to record PINs/passwords will be recorded, sealed, stored, and inventoried in accordance with procedures set forth in Article 515.f. and must be labeled with the following information:

(a) **Part 1/2**

Block 5 – enter Administrator/Operator UNIX account name.
Block 10 – enter name of Administrator/Operator.
Label top of form with: "LMD/KP SYS AD PIN/PASSWORD"

or

"LMD/KP SYS OP PIN/PASSWORD"

(b) **Part 2A**

Administrator/Operator UNIX account name.
KP PIN.
UNIX account password.

NOTE: For SF-700s protecting LCMS PINS or passwords, Part 1 will be classified SECRET unless the individual records their own personal PIN and password on a single SF-700. If so done and the persons PIN is privileged at the TS level, parts 2 and 2A of the SF-700 will be labeled and safeguarded at the TS level and must reflect the following derivative and downgrading instructions: "Derived from: 32 CFR 2001.80(d)(3)" "Declassify: Upon Change of Password or PIN".

(10) Classified COMSEC-related material not covered above must be safeguarded, stored and disposed on based on its classification in accordance with SECNAV M5510.36 (series).

(11) Unclassified COMSEC material not designated as CCI must be stored in a manner sufficient to preclude any reasonable chance of pilferage, theft, sabotage, tampering, or access by unauthorized persons.

(12) COMSEC material designated as CCI must be handled in accordance with Article 535.

NOTE: Classified magnetic media and printed matter must reflect the appropriate classification and downgrading instructions in accordance with Article 715, as required by SECNAV M5510.36.

525. PREPARING COMSEC MATERIAL FOR SHIPMENT:

a. **Packaging Materials/Shipment Containers**: Materials used for packaging COMSEC material for transportation must be strong enough to protect the material while in transit, prevent items from breaking through the container, and enable detection of any tampering.

b. **Wrapping Requirements**:

(1) Status markings must be removed from physical material prior to shipment. Shipment of COMSEC material with status markings intact is a Practice Dangerous to Security (PDS in accordance with Chapter 10.

(2) All COMSEC keying material and classified COMSEC material **must be** double-wrapped (using a non-transparent wrapper) and securely sealed.

(3) Unclassified COMSEC material other than keying material need only be wrapped once (using a non-transparent wrapper).

c. **Wrapper Marking Requirements**:

(1) Inner wrapper: The inner wrapper must be marked with the following information:

(a) Highest classification of the material.
(b) TO and FROM addressees.
(c) EKMS account number of the shipping & receiving unit
(d) CRYPTO or other special handling markings.
(e) Controlled package number.
(f) **"TO BE OPENED ONLY BY EKMS MANAGER."**

(2) Outer wrapper: The outer wrapper must be marked with the following information (applicable for shipments of all COMSEC material):

(a) "TO" and "FROM" addressees.
(b) Any applicable notation to aid delivery of the package.

NOTE: The outer wrapper must never reflect markings which indicate the article contains classified material, keying material or CCI.

(3) The manner in how the package must be addressed may vary slightly depending on the shipment method used. Use the following guidance as applicable:

(a) When transporting material via DCS, conform to DCS guidance on packaging requirements.

(b) Material transmitted by State Department diplomatic pouch must indicate that "**Courier Accompaniment Required.**"

(c) When using a commercial carrier to transport CCI, a complete address must be used (this includes the street address, building number, and zip code). Some commercial carriers may also require the telephone number of the receiving command to be on the address label of the package.

d. **Packaging and Shipping Restrictions**:

(1) Package keying material separately from its associated COMSEC equipment unless the application or design of the equipment is such that the corresponding keying material cannot be physically separated from it.

(2) Ship equipment with embedded COMSEC material the same way as keying material is shipped.

(3) Package primary and associated keying material (e.g., KW-46 BAV and UV) in separate packages within a shipment. Encrypted TEK and its associated KEK must be shipped in separate packages.

(4) COMSEC equipment must not be shipped in a keyed condition unless removal of the keying material is impossible.

(5) Batteries must be removed from COMSEC equipment (including FDs) unless the removal is impossible. To prevent software design devices from being received in a "Tampered State" and require reporting as a COMSEC Incident and return of the equipment to the vendor, batteries will not be removed from KG-175D, KG-250, Mark XIIA AIFF Mode 4/5 or other Software-Designed COMSEC devices prior to shipment as outlined in the applicable operational security doctrine for these devices can be found at:

http://iad.nsa.smil.mil/library/resources/library/index.htm under the "Doctrine" tab. SPAWAR has developed a listing of Software-Designed COMSEC devices which can be found at: https://infosec.navy.mil/crypto

(6) CIKs **must be** shipped separately from the associated equipment unless they are not yet initialized or are zeroized (disassociated) before shipping.

(7) PINS and/or passwords for equipment which make use of such for authentication must **NOT** be shipped with the equipment.

(8) When shipping keying material marked CRYPTO, packages will contain no more than four editions (for material that is superseded quarterly or more frequently) or two editions if the material is superseded semi-annually or annually. **This restriction does not apply to packaged irregularly superseded keying material and may be waived by NCMS//N5// when a new account is established or shipment options limited.**

(9) For physical material, if the quantity to be shipped exceeds that in paragraph (8), the material must be split into several packages and entered into DCS in staggered shipments that are not likely to be combined.

(10) There is no restriction on the number of short titles that can be enclosed in each package or the number of copies of an edition.

(11) The KP must be packaged and shipped via DCS separately from any of its associated CIKs or KSD-64As. The KP must be zeroized prior to shipment to the CMIO Broken Copy Account for maintenance or recertification. In the event the KP becomes inoperable and the operator is unable to confirm that the KP has been zeroized, do not ship any CIKS with the device and annotate on the transfer SF-153 "device could not be zeroized due to error XXXXXX (include the error code, if known or EKMS Help Desk

ticket #).

(12) Magnetic Media (e.g., removable media such as floppy disks, tape, etc.) containing encrypted key must be shipped separately from their associated Key Encryption Keys (KEKs). Magnetic media used to transport encrypted key must be marked "SECRET-COMSEC accountable" and must indicate whether or not EKMS transactions are on the media.

530. **TRANSPORTING COMSEC MATERIAL**:

The provisions of this article only apply to the physical movement between EKMS accounts. Movements within a command must be performed by properly cleared and authorized individuals. The authorized methods of transporting COMSEC material are discussed in this chapter. A quick reference matrix can be found on the following page.

COMSEC MATERIAL SHIPPING METHODS QUICK REFERENCE

Shipping Method	**Top Secret/ Secret material marked "crypto" or items with classified logic or algorithms**	**Confidential keying material marked "crypto"**	**Unclas keying material marked "crypto"**	**TS/Secret Equipment (not designated as CCI)**	**CCI (unclas, not keyed) (See Note 1 & 4)**
DCS	YES	YES	YES	YES	YES (OCONUS, when other approved methods are not available or will not meet mission requirement)
SDCS	YES	YES	YES	YES	YES
Designated and cleared couriers	YES	YES	YES	YES	YES
Commercial Carrier (**PSS/Ground**)	NO	YES	YES	YES	YES (**See Note 5**)
Commercial Carrier	NO	NO	YES (**See Note 2**)	NO	YES (**See Note 1**)
USTRANSCOM WWX-5	NO	NO	NO	NO	YES **(See Note 7)**

(**CONUS/OCONUS**)					
USTRANSCOM DESPS(**CONUS only**)	NO	NO	NO	NO	YES **(See Note 7)**
USPS (**Registered Mail**)	NO	YES	YES	NO	YES (**See Note 6**)
USPS (Express Mail)	NO	NO	NO	NO	YES (**See Note 3**)
Navy Supply System, Military Air (AMC, LOGAIR, QUICKTRANS, etc…)	NO	NO	NO	NO	YES

Figure 5-1

DCS = Defense Courier Service, DESPS = DoD Domestic Express Small Package Delivery Service, PSS = Protective Security Services, SDCS = State Department Courier Service, WWX-5 = World Wide Express 5, United States Postal Service = USPS. Registered Mail must not pass through a foreign postal system or be subject to foreign inspection. Material shipped to APO/FPO addresses does not pass through a foreign postal system.

Note: (1) See Article 535 for additional information, restrictions and notification requirements.

(2) See Article 530.a.3 for additional information and restrictions.

(3) The shipper must obtain assurance from U.S. Postal Service authorities that the material will receive continuous electronic or manual tracking to the point of delivery and a recipient‘s signature must be obtained. Material must be introduced into the postal system across-the-counter at a U.S. Postal Service Facility; the use of postal drop boxes are not authorized.

(4) Equipment which makes use of CIKS, PINS, or passwords is considered unclassified when these items are removed and shipped separately from the device. Devices should always be shipped in a zeroized state however, should mission requirements necessitate loading the device prior to shipment, associated CIKS, PINS, or passwords MUST be shipped separately. If any of these items are shipped with the equipment, it must be reported as a Physical Incident in accordance with Chapter 9.

(5) **Up to SECRET, CONUS ground only;** A list of commercial carriers offering PSS services may be requested from the Surface Deployment and Distribution Command (SDDC) via email from: sddc.ops.CarrReg@us.army.mil.

(6) The International Mail Manual (IMM) must be consulted prior to shipment of CCI containing lithium batteries to/from an APO/FPO address via registered mail.

(7) USTRANSCOM WWX-5 CONUS-OCONUS, OCONUS-CONUS USTRANSCOM DESPS within CONUS[1]

a. **Keying Material**:

(1) TOP SECRET and SECRET: All TOP SECRET and SECRET keying material marked or designated CRYPTO and items that embody or describe a cryptographic logic or algorithm must be transported by one of the following methods:

(a) USTRANSCOM Defense Courier Division[2].

(b) State Department Courier Service (SDCS).

(c) Formally cleared department, agency, or contractor individuals designated as couriers. TOP SECRET keying material must be handled in accordance with TPI standards. This is to include utilizing pilots/personnel of ships in company to transport TOP SECRET keying material.

NOTES: TPI is not required for TOP SECRET keying material in the custody of the DCS or SDCS but is required when picking up material from either and the accounts HCI is TS.

(2) CONFIDENTIAL: CONFIDENTIAL keying material marked or designated CRYPTO and items that embody or describe a cryptographic logic or algorithm must be transported by one of the following methods:

(a) Any method approved for TOP SECRET or SECRET keying material.

[1] Utilizes carriers and provisions in the USTRANSCOM DESPS contract as specified in the Defense Transportation Regulation (DTR 4500.9)

[2] Previously referred to as the Defense Courier Service (DCS)

(b) U.S. Postal Service, Registered Mail, provided the material does not pass through a foreign postal system or any foreign inspection. Mail to units serviced by the Army Post Office (APO) and Fleet Post Office (FPO) does not pass through foreign postal channels.

(c) Protective Security Services (PSS) is ground transportation (CONUS) provided by cleared commercial couriers who employ personnel with **up to SECRET** security clearances granted by the DOD and who are qualified by the Surface Deployment Distribution Command (SDDC). Additional information on PSS can be found at: http://www.sddc.army.mil and a list of PSS qualified carriers may be obtained from the SDDC, Carrier Services Branch at SDDC.OPS.CarrReg@us.army.mil.

(3) UNCLASSIFIED: Unclassified keying material marked or designated CRYPTO must be transported by one of the following methods:

(a) Any method approved for TOP SECRET, SECRET, or CONFIDENTIAL keying material; and

(b) UNCLASSIFIED keying material may also be transported using uncleared commercial carrier services may be used for provided each of the following is met:

1. The carrier provides continuous electronic tracking of the shipment equivalent to the tracking available through USPS registered mail.

2. A distant end receipt signature is provided.

3. The service is limited to shipments within the limits of the United States, its territories and possessions.

4. The carrier must be a firm incorporated in the United States.

5. The material to be transported is **strictly UNCLASSIFIED keying material.** Commercial carrier service is strictly forbidden for shipping any classified keying material marked or designated CRYPTO.

b. **COMSEC Equipment (less CCI):**

(1) TOP SECRET and SECRET:

(a) Any method approved for TOP SECRET or SECRET keying material.

(b) SECRET COMSEC equipment may also be shipped by cleared commercial carrier using PSS.

(2) CONFIDENTIAL (except key production equipment):

(a) Any method approved for TOP SECRET or SECRET.

(b) U.S. Military or military-contract air service (e.g., Air Force Mobility Command (AMC), LOGAIR, QUICKTRANS) provided that a continuous chain of accountability and custody (e.g., signature tally record) is maintained.

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

(3) UNCLASSIFIED: Unclassified equipment (**not designated CCI**) may be transported by any method approved for the transportation of equivalent high value/sensitive material. **When UNCLASSIFIED items or components are included with classified components, the method of shipment must be that required by the highest classification contained in the shipment.**

NOTE: See Article 535 for CCI shipping methods.

c. **Other COMSEC Material**: COMSEC material not covered above may be transported as follows:

(1) TOP SECRET material must be transported by DCS, SDCS, or cleared department, agency, or contractor courier.

(2) SECRET:

(a) Any method approved for TOP SECRET.

(b) Cleared commercial courier using PSS. Commercial carriers who employ personnel cleared **up to the Secret level** with DOD security clearances and provide PSS.

NOTE: Within CONUS, FTRs shipped separately from the associated device may be shipped as SECRET collateral using a GSA authorized carrier in accordance with SECNAV M5510.36.

(3) CONFIDENTIAL:

(a) Any method approved for TOP SECRET or SECRET.

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

(c) U.S. Military or military-contract air service (e.g., AMC, LOGAIR, QUICKTRANS) provided that a continuous chain of accountability and custody (e.g., signature tally record) is maintained.

(4) UNCLASSIFIED: Any means that will reasonably ensure safe and undamaged arrival at its destination.

d. **Use of Commercial Aircraft**:

1. Other than exceptions granted to military elements deploying or re-deploying on operational missions, COs, OICs, or SCMSROs are authorized, in cases of operational necessity, to approve the use of commercial aircraft to transport only that quantity of COMSEC material required to fulfill immediate, operational needs, provided:

(a) Transporation Security Administration procedures are followed.

(b) Couriers are appropriately cleared, possess written authorization (DD-2501) and briefed on their responsibilities.

2. Direct flights should be used and unless operationally necessary, do not transport keying material in aircraft over hostile territory.

3. U.S. flag aircraft can be used to courier COMSEC material within CONUS (includes Alaska, Guam, Hawaii, Puerto Rico and U.S. territories/possessions).

4. Transportation of COMSEC material outside of CONUS on a non-U.S. flag or any foreign-owned, controlled, or chartered aircraft, is strongly discouraged because of the threat by terrorists and the lack of U.S. control. When such is required to satisfy urgent mission requirements, second echelon or higher approval must be requested (i.e. TYCOM, FLTCDR, or Service Headquarters). The request must include an itinerary that

identifies the specific airline(s) to be used; whether the flight is non-stop or whether any intermediary stops may be required; and the estimated times of departure and arrival.

(a) In addition to having the written authorization in the form of official travel orders or a DD-2501, the courier must possess any customs documents needed to permit the material to enter the destination country and, when necessary, to permit the material to re-enter the U.S. Applicable forms issued by the Department of State for this purpose are:

(1) Form DSP-5, Application/License for Permanent Export of Unclassified Defense Articles and Related Technical Data, and

(2) Form DSP-73 Application/License for Temporary Export of Unclassified Defense Articles. (See http://www.pmddtc.state.gov/licensing/forms.html)

NOTE: Couriers who may be subject to customs inspection should contact their cognizant security authority to obtain the necessary customs documents.

(b) In unique travel circumstances (e.g., unexpected travel delays) COMSEC equipment and keying material may be kept under personal custody (e.g., overnight in a hotel) if authorized secure storage facilities are not available. In such circumstances, travelers must utilize government quarters (on base), if available, maintain continuous control of the materials at all times and attempt to reach their security officer for guidance.

e. **Use of Private Conveyances**: Unless prohibited by local, ISIC or TYCOM directives, either private or corporate-owned conveyances (e.g., POV, rental cars) can be used to transport COMSEC material **when a government vehicle is not available.** 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.

f. **Courier Responsibilities**: Courier personnel, including government, military or contractor personnel must have current, written authorization in the form of official travel orders or a DD-2501 from their organization. The authorization must be retained on the person at all times when performing duties of a courier and courier personnel must receive written instructions for safeguarding the material entrusted to them. The following provisions, at a minimum, must be adhered to:

(1) When hand-carrying COMSEC material, couriers must maintain constant personal custody of all keying material.

(2) 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. 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.

(3) Couriers must ensure all inspections are conducted in their presence and only by authorized personnel. External viewing and standard airport x-raying of equipment and protectively packaged keying material is permitted. In no case will U.S. COMSEC material be entered into foreign distribution channels, unless, authorization is granted by the NSA Foreign Affairs Directorate, IAD Operations Group.

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

(5) When transporting COMSEC material outside of CONUS, couriers must have the telephone number of the nearest U.S. Embassy or Consulate for every country that the aircraft is scheduled to fly through/to.

(6) Notify the recipient, in advance, of the flight itinerary and estimated time of arrival so that appropriate steps may be taken if the courier does not arrive within a reasonable amount of time after the flight has arrived.

(7) Be provided specific instructions for emergency situations, including loss or other compromise of the material they are carrying.

(8) Couriers may hand carry keyed COMSEC equipment containing key provided CIKs, PINs, and other activating sources for the equipment are removed/disabled and carried separately. (“Separately” means that the same individual courier may carry the CIKs, PINs, or other activating sources on their person, but not in the same package as the equipment itself). Couriers may hand carry keyed COMSEC equipment that does not have CIK/PIN capability with proper justification and written authorization from cognizant security officials.

g. **Restrictions on DCS Shipments**: In accordance with DOD Directive 5200.33, the following types of material may be sent through the DCS:

(1) CLASSIFIED:

(a) COMSEC material.

(b) Cryptologic material.

(c) Imagery material (Secret or higher).

(2) UNCLASSIFIED:

(a) Keying material marked or designated CRYPTO.

(b) CCIs outside the 48 contiguous states when no other means of secure transportation is available.

NOTE: If uncertain regarding what materials qualify, are prohibited, or other possible DCS restrictions consult the DCS Customer Service Manual.

h. **Airdrop of COMSEC Material**:

Unless precluded by system doctrine or handling instructions, and when operationally required, COMSEC material may be air-transported and air-dropped provided the following requirements are met:

(1) A properly cleared person controls the material until it leaves the aircraft.

(2) Every reasonable precaution is taken to ensure that authorized persons immediately recover the material.

(3) COMSEC material is not air-transported over hostile territory except in cases of operational necessity.

NOTE: Vehicles or shelters in which COMSEC Equipment is installed may be transported by helicopters using sling-loaded techniques, but the COMSEC equipment should not be keyed unless there is an operational requirement for the immediate operational use of the equipment upon landing. COMSEC aids may be carried inside the same helicopter, but must not be sling-loaded.

i. **Over-the-Air Rekey (OTAR), Over-the-Air-Distribution (OTAD) and Over-the-Air-Transfer (OTAT):**

a. **OTAR:** NCSs and Circuit Control Officers are authorized to conduct OTAR with key obtained through normal channels or is locally generated, and rekey remote circuits under their control that employ crypto systems designated for OTAR.

b. **OTAD/OTAT:** When authorized by the Controlling Authority of the key, Net Control Stations, Circuit Control Offices (CCO) and Operational Commanders are authorized to transmit key to required units using existing secure circuits which employ cryptosystems designated for OTAD/OTAT.

c. In an emergency, when prior Controlling Authority approval cannot be obtained without potential disruption to mission essential communications, the CO may authorize OTAD/OTAT of key to authorized holders. The CONAUTH must be notified of the key passed and unit such was provided to ensure the unit is notified in the event a Hazardous Condition (HAZCON) or Emergency Supersession is directed by the Controlling Authority.

d. **Except during an actual COMSEC emergency, the Key Encryption Key (KEK) used to protect key passed via OTAD or OTAT must be equal to/higher in classification than the Traffic Encryption Key (TEK) protected.**

e. OTAR/OTAD/OTAT procedures are contained in NAG-16.

f. See Chapter 11 for documentation, accounting, and destruction requirements for key transmitted, received or relayed electronically.

535. CONTROLLED CRYPTOGRAPHIC ITEM (CCI)

a. **Definition**: The definition of CCI can be found in Annex A.

b. **Accountability**: CCI is centrally accountable in the CMCS to the COR by serial number (ALC 1) or quantity (ALC 2). See Article 733.h **for service-specific differences in CCI accounting and their effect on inter-service transfer of CCI.**

c. **General Access Requirements**:

(1) A security clearance is not required for access to

unkeyed CCI. Normally, access must be restricted to U.S. citizens whose duties require such access.

(2) Unkeyed CCI and/or CCI keyed with unclassified key marked or designated CRYPTO, must be stored in a manner that affords protection against pilferage, theft, sabotage, or tampering, and ensures that access and accounting integrity are maintained.

d. **Access Requirements for Resident Aliens**:

Resident aliens who are U.S. Government employees, U.S. Government contractor employees, or National Guard, active duty, or reserve members of the U.S. Armed Forces may be granted access to CCI provided their duties require access.

e. **Access Requirements for Foreign Nationals**:

Non-U.S. citizens who are employed by the U.S. Government at foreign locations where there is a significant U.S. military presence (two or more military bases) may handle CCI material in connection with warehouse functions, provided they are under the direct supervision of an individual who has been granted access to CCI material.

(1) Access to Unkeyed CCI: Access may be granted to Foreign Nationals under the following conditions:

(a) In conjunction with building maintenance, custodial duties, or other operational responsibilities that were performed by unescorted personnel in the area prior to the installation of the CCI.

(b) The CCI is installed within a U.S. controlled or combined facility with a permanent U.S. presence, as opposed to a host nation facility.

(c) Command security authority has determined that the risk of tampering with the CCI, which could result in compromise of U.S. classified or sensitive classified information, is acceptable in light of the local threat, perceived vulnerability, and the sensitivity of the information being protected as indicated by its classification, special security control, and intelligence life.

(d) The Operational Security Doctrine for the CCI does not specifically prohibit such access.

(2) Access to Keyed CCI: The access requirements listed above for unkeyed CCI also apply to keyed CCI with the following additional restrictions:

(a) The non-U.S. citizens are civilian employees of the U.S. Government and are assigned to a combined facility.

(b) The non-U.S. citizens hold a clearance at least equal to the highest level of the keying material or information being processed.

(c) The CCI material remains U.S. property and a U.S. citizen is responsible for it. The presence of such installed CCIs must be verified at least monthly and the verification documented and retained in accordance with local command policy.

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

(e) U.S. users communicating with such terminals are made aware of the non-U.S. citizen status of the CCI user.

NOTES: 1. Waivers to permit unescorted access by non-U.S. citizens to installed CCIs under the conditions listed above must be submitted to NCMS//N5//.

2. Non-U.S. citizens in countries reflected in 22 Code of Federal Regulations (CFR) International Traffic In Arms Regulation (ITAR), ITAR Part 126 (General Policies and Provisions) **may not be granted access to installed CCI equipment without approval from DIRNSA//DP021//; submit requests via the Chain of Command to NCMS//N5//.**

f. **Keying CCI**:

(1) Only properly cleared and designated U.S. citizens are authorized to key CCI with classified U.S. key. Waivers of this policy must be authorized by NCMS//N5//.

(2) Non-U.S. personnel are authorized to key CCI using only Allied key or unclassified U.S. key.

g. **Classification of CCI When Keyed**:

When keyed, CCI assumes the classification of the keying material it contains, and must be handled in accordance with the control and safeguarding requirements for classified keying material described in this manual.

> **Note: Most newer CCI equipment make use of CIKS, PINS or passwords to permit or prohibit access to the contents or use of the device. Unless otherwise stated in the respective Operational Security Doctrine, when CIKS are removed and stored separately or PINS and passwords are not entered, these devices will be stored and safeguarded as unclassified CCI.**

h. **Installing CCI in a Foreign Country**:

When there is an operational necessity to install and operate a CCI in a foreign country at a facility that is either unmanned or manned entirely by non-U.S. citizens, the installation must be approved, in advance, by NCMS//N5//.

(1) In addition to the requirements listed above, special security measures will be required (e.g., constructing vault areas, storing CCI material in approved security containers, installing alarm systems) to prevent unauthorized access to the CCI by non-U.S. citizens.

(2) The installation of the CCI must be accomplished and controlled by U.S. citizens who shall verify the presence of the CCI equipment at regular intervals.

i. **Moving CCI to a Sensitive Environment**.

CCI material should not be moved from an environment where the risk of tampering by foreign nationals is acceptable, to a more sensitive environment where the risk of tampering by foreign nationals is not acceptable.

(1) When operational requirements necessitate moving CCI to a more sensitive environment, the command must send a message to NCMS//N5// requesting authorization to move the material.

(2) Before moving the CCI, it must be examined for signs of tampering by qualified COMSEC maintenance personnel.

(3) Report any evidence or suspicion of tampering to DIRNSA//I31132// as a COMSEC incident in accordance with Chapter 9. The affected CCI equipment shall be removed from operational use pending disposition instructions from DIRNSA.

j. **Transporting Keyed/Unkeyed CCI**:

(1) CCI must not be shipped in a keyed condition unless removing the key is impossible.

(2) Unkeyed CCI may be shipped/transported by any means delineated in Article 535.k or 535.l, as applicable.

k. **Methods of Shipping CCI**. CCI equipment must be shipped only to authorized activities using any of the following methods:

(1) Authorized U.S. Government department, service, or agency courier (e.g., Navy Supply System).

(2) Authorized U.S. Government Contractor/Company or U.S. citizen courier.

(3) U.S. Postal Service Registered mail or express mail, provided the material does not at any time pass out of U.S. postal control, pass through a foreign postal system, pass through any foreign inspection, or otherwise fall under the control of unescorted foreign nationals. When using express mail, the shipper must obtain assurance from U.S. Postal Service authorities that the material will receive continuous electronic or manual tracking to the point of delivery. A recipient's signature must be obtained. Material must be introduced into the postal system "across-the-counter" at a U.S. Postal Service Facility; postal drop boxes must not be used.

NOTES: 1. There are certain restrictions governing the size and weight of packages that can be shipped via registered mail. Prior to shipping the CCI, check with the postal service to determine whether the shipment qualifies.

2. First, fourth, certified, insured and parcel post are not authorized methods of shipping CCI equipment.

(4) Commercial carriers (non-military aircraft) may be used to transport CCI (includes CCI being transported in conjunction with Foreign Military Sales) within the U.S., its territories, and possessions, providing the carrier warrants in writing the following:

(a) It is a firm incorporated in the U.S. that provides door-to-door service.

(b) Guarantees delivery within a reasonable number of days based on the distance to be traveled.

(c) Possesses a means of tracking individual packages within its system to the extent that should a package become lost, the carrier can, within 24 hours following notification, provide information regarding the last known location of the package(s).

(d) Guarantees the integrity of the vehicle's contents at all times.

(e) Guarantees that the package will be stored in a security cage should it become necessary for the carrier to make a prolonged stop at a carrier terminal.

(f) Utilizes a signature/tally record (e.g., a carrier's local signature/tally form or the DD Form 1907 or Form AC-10) that accurately reflects a continuous chain of accountability and custody by each individual who assumes responsibility for the shipment while it is in transit;

OR

1. Utilizes an electronic tracking system that reflects a chain of accountability and custody similar to that provided by a manually prepared signature/tally record.

2. Ensures positive identification of the actual recipient of the material at the final destination.

3. Uses a hard-copy printout that serves as proof of service; the printout must reflect those points, during transit, where electronic tracking of the package or shipment occurred.

(5) U.S. military, military-contractor, or private air service (e.g., AMC, DESPS, LOGAIR, QUICKTRANS, WWX-5), provided the carrier satisfies the requirements identified above for commercial non-military aircraft carriers.

(6) U.S. Diplomatic Courier Service.

(7) DCS outside CONUS, when no other methods of secure transportation are available. Prior authorization must be obtained from DCS before any unkeyed CCIs are introduced into the DCS system.

(8) Commercial passenger aircraft may be used within the U.S., its territories, and possessions. Transport of CCI material outside the U.S., its territories, and possessions on a non-U.S. flag or any foreign-owned, controlled, or chartered aircraft is strongly discouraged because of the threat of terrorists and the lack of U.S. control. When such is required to satisfy urgent mission requirements, second echelon or higher approval must be requested (i.e. TYCOM, FLTCDR, or Service Headquarters). The request must include an itinerary that identifies the specific airline(s) to be used; whether the flight is non-stop or whether any intermediary stops may be required; and the estimated times of departure and arrival.

(a) In addition to having the written authorization in the form of official travel orders or a DD-2501, the courier must possess any customs documents needed to permit the material to enter the destination country and, when necessary, to permit the material to re-enter the U.S. Applicable forms issued by the Department of State for this purpose are:

(1) Form DSP-5, Application/License for Permanent Export of Unclassified Defense Articles and Related Technical Data, and

(2) Form DSP-73 Application/License for Temporary Export of Unclassified Defense Articles. (See http://www.pmddtc.state.gov/licensing/forms.html)

NOTE: Couriers who may be subject to customs inspection should contact their cognizant security authority to obtain the necessary customs documents.

(b) In unique travel circumstances (e.g., unexpected travel delays) COMSEC equipment and keying material may be kept under personal custody (e.g., overnight in a hotel) if authorized secure storage facilities are not available. In such circumstances, travelers must utilize government quarters (on base), if available, maintain continuous control of the materials at all times and attempt to reach their security officer for guidance.

NOTE: Requirements/restrictions for shipping CCI on commercial aircraft are discussed below.

(9) Non-U.S. citizens who are employed by the U.S. Government at foreign locations where there is a significant U.S. military presence (two or more military bases) may

transport CCI material, provided there is a signature record that provides continuous accountability for custody of the shipment from the time of pick-up to arrival at the final destination.

NOTE: A U.S. citizen must accompany the foreign driver carrying the material or the material must be contained in a closed vehicle or shipping container (e.g., CONEX, DROMEDARY, or similar authorized container) which is locked with a high security lock and contains a shipping seal that will prevent undetected access to the enclosed material.

l. **Requirements and Restrictions for Transporting CCI on Commercial Aircraft**:

Note: The provisions of this article are intended to supplement those set forth in Article 530.d above.

(1) The container(s) and content(s) may be subject to certain security inspections, including x-ray, by airport personnel. Inspections are permissible, but only in the presence of the courier.

(2) Inspection of CCI material must be restricted to exterior examination only and conducted in the presence of the courier. To preclude unnecessary inspections by airport personnel, couriers should carry current orders, letters, and ID cards identifying them as designated couriers.

(3) CCI material must be stored in the cabin of the aircraft where the courier can maintain continuous control of the material.

(4) When the size of the CCI shipment is too large for storage in the cabin of the aircraft, the entire shipment must be packaged in a suitable container, which is secured and sealed in such a manner so that any unauthorized access to the enclosed CCI can be detected by the courier. The CCI shipment may then be shipped as checked baggage, provided the last-in, first-out (LIFO) procedure is coordinated with the carrier.

m. **Storage of CCI**: Unkeyed CCI and/or CCI keyed with unclassified key marked or designated CRYPTO, must be stored in a manner that affords protection against pilferage, theft, sabotage, or tampering, and ensures that access and accounting integrity are maintained.

n. **Packaging CCI**: Package unkeyed CCI for shipment in a manner that will allow for tamper detection and prevent damage while in transit.

(1) In addition to the information required on the packaging label, include the office code or duty position title of the individual who is designated to accept custody of the CCI equipment to ensure proper delivery. Do not use the name of an individual.

(2) The shipping document must also contain an emergency telephone number(s) for the intended recipient in the event delivery is made after normal working hours.

o. **Notification of Shipment to Intended Recipient**:

Regardless of the method used to transport CCI, the transferring command must, within 24 hours of shipping, notify the intended recipient of the method of transportation and a list of CCI(s) that have been shipped.

p. **Shipments not Received**:

(1) If a shipment of CCI equipment has not been received within five working days after the expected delivery date, contact the originator of the shipment immediately.

(2) Upon being notified of the non-receipt, the originator of the shipment will initiate tracer action and include NCMS//N3// as an info addressee on all tracer actions. If the location of the shipment cannot be determined, the material shall be assumed lost and the incident must be reported in accordance with Chapter 9.

q. **Reportable Incidents**:

(1) Lost shipments, shipments that show evidence of possible tampering, and unauthorized access to CCI equipment must be reported to DIRNSA//I31132//, info NCMS//N5//.

(2) All other incidents involving improper shipping or handling of CCI equipment must be reported to NCMS//N5//, info DIRNSA//I31132//. If a commercial carrier is involved, include the name(s) of the carrier(s).

540. ROUTINE DESTRUCTION OF COMSEC MATERIAL:

a. **General**: Effective and superseded keying material is extremely sensitive, and if compromised, potentially exposes all of the information encrypted by it to compromise. For this reason, keying material (other than defective or faulty key) must be destroyed as soon as possible after it has been superseded or has otherwise served its intended purpose. COMSEC key is destroyed when it is superseded (usually as a result of regular supersession), when it is expired, or when receipt of specific direction to destroy the key (e.g., emergency supersession) is received.

NOTE: Failure to destroy COMSEC material within the timeframes outlined in this article is considered a COMSEC Incident in accordance with Chapter 9.

b. **Categories of COMSEC Material**: The various categories of COMSEC material discussed below are detailed in Article 260 and should be reviewed to ensure compliance with the destruction requirements contained in this chapter.

c. **Destruction Personnel**: COMSEC material that is authorized for destruction must be destroyed by two properly cleared and authorized personnel, in accordance with this guidance:

(1) Destruction of hard copy or physical COMSEC material:

(a) When unissued (i.e., retained in the account vault or safe of the EKMS Manager or LE (Issuing)), superseded COMSEC material must be destroyed by the EKMS Manager or Alternate and a properly cleared EKMS witness.

(b) When issued to LEs (Using), superseded COMSEC material must be destroyed by two properly cleared and authorized personnel.

(2) Destruction of Electronic COMSEC material **within LCMS**:

(a) LCMS provides the ability to view all expired modern (asymmetric) or superseded traditional (symmetric) electronic keying material. The data in LCMS can be filtered to aid in ensuring timely and proper destruction of expired or superseded keying material.

Note: EKMS Managers must keep in mind status information changes and is influenced by things such as emergency supersession which generally has a cascading effect on

future editions. The status information applied to physical material held at the account or electronic key stored on the LMD may be inaccurate and should always be verified prior to affecting any destruction, especially when assuming responsibility for an account.

1. For normal end of month destruction, both superseded and expired key must be destroyed. The EKMS 704 (series) LMD/KP Operators Manual provides step-by-step guidance in preparing destruction reports and destroying electronic key at the account level.

2. A single Manager or Alternate can destroy electronic key stored on the LMD. A witness is not required as the activity and person who conducted the action is retained in the LCMS Activity Data.

3. Modern key loaded by LE personnel must be deleted from the device storing the key and the destruction reported to the EKMS Manager who will record the key(s) loaded using the "Record Filled in End Equipment" feature in LCMS.

4. When the "Record Filled in End Equipment" feature is used or the EKMS Manager or Alternate "Directs Destruction of Own Electronic Key" at the account level, there is no working copy of a destruction report created by LCMS. The items "Recorded as Filled in End Equipment" will appear on the next Reportable or Local Destruction report generated at the account.

5. For traditional electronic key (Reg 00 keying material), although the Manager may direct destruction of the Short Title/Edition at the account level in LCMS, if the Short Title and Edition is reflected in LCMS as "issued", until the respective LE destroys the keying material, reports it to the account and the LE destruction report is confirmed by the Manager, it will not appear on the account's end of month report. In LCMS, all copies of Reg 00 key must be accounted for or recorded as destroyed for it to be confirmed and appear. Should the manager originate a reportable and/or local destruction record prior to confirming all LE destruction reports, the Manager will have to confirm, after the fact the remaining reports and originate another reportable and/or local destruction report for the CO to sign NLT the 5th working day of the month. **If noted afterwards, it must be documented as a COMSEC Incident (late destruction).**

NOTE: In the event of a system failure that requires

restoration from a back-up tape, any key (electronic and physical) that was destroyed since the last back up was conducted will re-appear in the account or on AIS (physical). Previously destroyed key must be destroyed as soon as possible after the restoration and always within the timeframes of this article. Failure to do so must be documented and reported IAW Article 945.

(3) Destruction of electronic material **outside of LCMS**:

(a) Destruction of keys issued to a DTD, SKL, TKL is accomplished through either deletion or zeroizing the device, if no longer required. Audit trail reviews provide the required verification the key was destroyed negating the requirement for a hard copy CMS-25 destruction report unless required by local, ISIC or TYCOM policy. The material will appear on a working copy of a destruction report, when issued to a LE. Two properly cleared LE personnel must verify the key(s) on the end of the month destruction report have been deleted from the device prior to signing and returning the SF-153 to the EKMS Manager. The EKMS Manager, Alternate or properly cleared and authorized Supervisory User/SSO at the LE level will verify destruction during the audit trail review which must be documented.

(b) Destruction of electronic keys in other common fill devices (KYK 13, KYX 15) which do not possess audit capability must be witnessed by **two** properly cleared and authorized persons. Key destroyed from these devices which were passed/received via OTAD/OTAT will be reflected as destroyed, when superseded and the slot zeroized and verified in the OTAD/OTAR/OTAT log.

d. **Conditions Affecting Keying Material Destruction**: The destruction requirements for keying material will vary depending on several factors; for example:

(1) Whether or not the keying material is marked or designated CRYPTO,

(2) Whether it has been issued to LEs (Using), or,

(3) Whether it remains unissued (i.e., in the EKMS Manager or LE (Issuing) vault or safe, etc.). Accordingly, these factors and how they affect the 12-hour standard are identified in the Routine Destruction and Emergency Supersession exceptions stated in paragraphs e. and f. below.

e. **Routine Destruction of Regularly and Irregularly Superseded Keying Material**: Destroy immediately after use when more than one copy of the key setting is available, or as soon as possible after the cryptoperiod and always within 12 hours after the end of the cryptoperiod. **Exceptions** to the 12-hour destruction standard are as follows:

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

(2) Superseded keying material on board an aircraft is exempt from the 12-hour destruction standard but must be destroyed as soon as practicable upon completion of airborne operations.

(3) Superseded segments of sealed segmented/ extractable keying material (unissued or issued) need not be destroyed until the entire edition is superseded or the keying material is unsealed, whichever occurs first. When retained until the entire edition is superseded, this guidance applies:

(a) Unissued: destroy no later than 5 working days after the month in which supersession occurs.

(b) Issued: destroy no later than 12 hours after the entire edition supersedes.

NOTE: "Sealed keying material" is defined as that which either remains unopened in its original protective packaging or has been resealed in accordance with Article 772. Canister-packaged keying material is considered sealed, even after initial use (one or more segments have been removed from the canister for use). Accordingly, superseded segments need not be removed and destroyed until an effective segment is required for use or until the entire edition is superseded, whichever occurs first.

(4) Issued keying material packaged in canisters containing multiple copies of each segment (e.g., 1/01,1/02, 1/03 etc.):

(a) Destroy all copies except the last copy immediately after use.

(b) Retain the last copy of each effective segment until the cryptoperiod expires, then destroy within 12 hours.

(5) Issued codes (e.g., AKAC 874) consisting of sections that are used incrementally (e.g., 6-hour periods). Destruction of each 6-hour section need not be carried out until the entire table or page is superseded. Users have 12 hours from the time the entire table or page supersedes to complete destruction.

(6) Keying material that supersedes at intervals of less than one month (e.g., 7-, 10-, and 15-day codes):

(a) Unissued: The keying material may be held until the next end of the month destruction, but must be destroyed no later than five working days after the end of the month in which the edition was superseded.

(b) Issued: Do not open security containers for the sole purpose of performing routine destruction. However, if the security containers are opened for any reason and LEs (Using) must unseal the material to remove an effective segment for use, all previously superseded segments must then be destroyed.

(7) Irregularly superseded keying material whose supersession is promulgated by message must be destroyed as follows:

(a) Unissued: The keying material may be held until the end of the month destruction but must be destroyed no later than five working days after the month in which supersession occurs.

(b) Issued: Destroy as soon as possible after receipt of the supersession message and always within 12 hours of receipt of the message.

(8) Superseded COMSEC material received in an ROB shipment must be destroyed as soon as possible but always within 12 hours of opening the shipment. Annotate on the SF-153 destruction document, "**SUPERSEDED ON RECEIPT.**" No additional reporting is required.

(9) Destroy irregularly superseded training/maintenance keying material when it becomes physically unserviceable.

(10) Destroy on-the-air test key at the end of the testing period as determined by the test director.

(11) If material is involved in an investigation, specific instructions to retain the material beyond its supersession date will be provided by NCMS//N5// or DIRNSA//I31132//.

(12) To permit processing of message traffic received after the effective cryptoperiod of a key, keying material for all auto manual off-line systems (e.g., KL-42, KL-43, KL-51, AN/PYQ-20 or later devices intended for off-line encryption) may be retained up to, but no longer than, 72 hours after supersession.

(13) GPS keying material may be retained and used for up to 12 hours after the regularly scheduled supersession period to comply with the NAVSTAR GPS Selective Availability and Anti-Spoofing Host Application Equipment Design Requirements with the Precise Positioning Security Module (SAASM). A copy of the related approval letters can be found on the NCMS SIPR site under the EKMS Managers Tab – GPS Approval Letters. See Annex S for the new URL. Additionally, NSA-GPSSOPO-0343 authorizes the use of three consecutive GPS keys during the 12-hour period following the first key's regular supersession period.

f. **Emergency Supersession of Keying Material**. When involved in compromise situations, destroy superseded material as soon as possible and always within 12 hours of receipt of emergency supersession notification. The only exceptions to this 12-hour destruction standard are as follows:

(1) In the case of an extended holiday period (over 72 hours) or when special circumstances prevent compliance with the 12-hour standard, destruction may be delayed until the next duty day. In such cases, destruction must be conducted as soon as possible after reporting for duty.

(2) When a segment of issued canister-packaged keying material is emergency superseded before its cryptoperiod, comply with the following:

(a) Do not remove the emergency superseded segment from the canister for destruction until all segments preceding the superseded segment have been used or destroyed.

(b) Until such time as the emergency superseded segment(s) can be removed from the canister for destruction, adhere to the following procedures to prevent accidental use of the superseded segment:

1. Place the affected canister in a Zip Lock bag along with a copy of the message directing emergency supersession of the segment(s), **OR**

2. Wrap a copy of the supersession message securely around the canister using a rubber band.

Note: The procedure in Para (2) above does not apply to electronic key in a DTD, SKL, and TKL. To prevent the potential for a cryptographic incident and possible adverse mission impact, if an individual segment is emergency superseded and held in electronic form in a DTD, SKL, TKL, etc…it will be destroyed within 12 hours of receipt of the message or next duty day (for a non-watch environment).

(c) When a segment of unissued canister-packaged keying material, is emergency superseded before its cryptoperiod, comply with the following:

1. Follow the procedures described above for issued canister-packaged keying material or hold the unissued canister for routine end of the month destruction.

2. When held until the end of the month, the Manager must ensure that the keying material is destroyed no later than five working days after the month in which supersession of the entire edition occurs.

(3) When unissued keying material protectively packaged in other than canisters is emergency superseded, comply with the following:

(a) Destroy superseded segments immediately or hold the unissued keying material edition for routine end of month destruction.

(b) To prevent accidental use of superseded segments, wrap/attach a copy of the supersession message securely (e.g., using a rubber band) around the remainder of the material.

(c) When held until the end of the month, the Manager must ensure that the keying material is destroyed no later than five working days following supersession of the entire edition.

g. **Destruction of Maintenance Manuals, Operating Instructions, and General Doctrinal Publications**:

(1) Destroy within five working days after the end of the month in which superseded.

(2) Residue of classified and unclassified amendments to these publications must be destroyed as soon as possible, but no later than five working days after entry of the amendment.

h. **Destruction of COMSEC Equipment**: Unless otherwise directed by NCMS//N3//, COMSEC equipment will **NOT** be destroyed at the local command level, but will be disposed of as directed by NCMS. The following guidance pertains:

(1) When authorization to destroy COMSEC equipment has been received by an account from NCMS//N3// and a deadline destruction date has not been identified:

(a) Destroy within 90 days of receipt of the destruction authorization. If destruction cannot be accomplished within this specified timeframe, the account must request a waiver from NCMS//N3/N5// identifying material involved, authorization message date-time-group, circumstances as to why the account cannot comply, and anticipated date of destruction.

(b) Accounts that fail to destroy material within the 90 day timeframe and have not requested a waiver are in violation of CMS policy and must document a "late destruction" COMSEC Incident in accordance with Chapter 9.

(2) Do not destroy COMSEC equipment that is being used on a particular net until all users are up and operational on the replacement equipment. Therefore, accounts must exercise caution to ensure no degradation in communications occurs when changing from one secure system to another.

(3) COMSEC equipment identified for destruction will remain on an account's inventory until the destruction has been carried out and reported to the COR.

(4) Questions concerning COMSEC equipment destruction, other than that indicated, may be referred to NCMS//N3//.

(5) For material that is to be demilitarized or returned to the NSA Classified Material Conversion (CMC), always consult and adhere to the CMC guidance for preparation of materials, limits and documentation requirements.

i. **Reporting Destruction**: Report destruction in accordance with the guidance contained in Chapter 7 or as directed by NCMS.

j. **<u>Routine Destruction Methods</u>**:

1. Only devices and methods approved by NSA, as reflected on the NSA Evaluated Products List (EPL) will be used for terminal destruction of COMSEC material. NSA promulgates guidance for various types of media containing COMSEC material. Click here for the latest version of the EPL.

2. A quick reference matrix is contained in this chapter to reflect methods approved for destroying COMSEC material. Related narrative remains in this chapter for residue size limits and other guidance, including safety precautions.

NOTES: 1. For the purposes of this Article, *terminal destruction* is defined as the *complete* destruction of material by authorized means such that recovery and reconstruction of the original material is impossible.

2. Keymat in canisters (key tape) is <u>not</u> paper COMSEC material, rather it is a blend of paper and polyester otherwise known as "Mylar©" or, in NSA-originated documents, as "PMP (Paper-Mylar-Paper)" Authorized destruction methods for key tape are addressed in Article 540 under *Non-paper* COMSEC material.

COMSEC MATERIAL DESTRUCTION QUICK REFERENCE

Material	**Burn**	**Shred**	**Pulp**	**Chemical Means**	**NSA approved disintegrator**	**Degauss or Overwrite**	**Remarks**
Paper COMSEC and Classified Material, i.e. (AKAIs, AKACs, AMSHs, USKACs)	**Yes**	**Yes**	**Yes**	**No**	**Yes**	**NA**	If local policy permits burning however, it must be reduced to white ash and contained to prevent loss of unburned pieces of material. Ashes must be inspected, broken up or reduced to sludge. **Only NSA-approved cross-cut shredders may be used.** For pulping must be broken down to non-legible fiber residue.
Canister Packaged Keying Material	**Yes**	**No**	**No**	**No**	**Yes**	**NA**	**For burning, see above.** Always punch holes in the canister; inspect it for any segments that may have not been completely extracted and destroyed; Remove and shred any barcode labels found to still be applied and inspect the destruction device and bag before disposal to prevent recovery of any undestroyed material.
Microfiche	**Yes**	**No**	**No**	**Yes**	**Yes**	**NA**	For burning or disintegration, see above. For chemical usage (bleach, acetone, methylene chloride) immerse for 5 minutes, separate film sheets
Floppy Disks	**Yes**	**Yes**	**NA**	**NA**	**Yes**	**Yes**	Floppy Diskettes must be removed from the casing. If shredded residue must not exceed 5mm in size.
CD/DVD	Always consult the latest NSA guidance on the destruction of optical media.						
Classified Hard Drives	See the NSA/CSS Storage Device Declassification Manual and Naval Telecommunications Directive (NTD) 03-11.						
COMSEC Equipment (CCI)	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	If authorized, must be destroyed in accordance with EKMS-5A and the NSA Equipment Demilitarization Process.

Figure 5-2

(1) *Paper* COMSEC Material: Destroy paper COMSEC material by burning, crosscut (double-cut) shredding, or pulping in authorized devices.

(a) When burning, the combustion must be complete so all material is reduced to white ash and contained so that no unburned pieces escape. Inspect ashes and break up or reduce to sludge, if necessary.

1. Placing material in a burn bag does not constitute destruction. Destruction is the actual destruction by burning, shredding, or other authorized means that makes recovery or reproduction impossible.

2. Do not transport burn bags of *un-shredded* COMSEC keying material to destruction facilities outside the jurisdiction of the command unless controlled by the EKMS Manager and/or Alternate and a qualified EKMS witness.

(b) Pulping (wet process) must break down the material to non-legible fiber residue (5mm).

(c) Cross-cut shredders are only authorized for paper COMSEC material and are not authorized for canister packaged keying material. NSA-approved shredders are reflected on the EPL.

(2) *Non-paper* COMSEC Material: Destroy by burning, melting, disintegration, or chemical alteration (e.g., use of acetone or methylene chloride) until it is decomposed to such a degree that there is no possibility of reconstructing key, keying logic or classified COMSEC information by physical, electrical, optical, or other means.

NOTES: 1. For the purposes of this article, *terminal destruction* is defined as the *complete* destruction of material by authorized means such that recovery or reconstruction of the original material is impossible.

2. Keymat in canisters is not paper COMSEC material; it is a blend of paper and polyester otherwise known as "Mylar" or "PMP."

(a) With exception to emergency destruction, if directed, canister-packaged keying material (PMP) will only be destroyed through disintegration using a NSA-approved disintegrator or through burning as described above for paper COMSEC material. A listing of NSA-approved High Security disintegrators can be found here. For canister packaged material, puncture empty key tape canisters on both sides of the canister and dispose of it as unclassified material. Ensure that the canister is empty before disposing of it.

(b) Microfiche, microfilm, or other reduced-image photo negatives will be destroyed as follows:

1. Before burning microfiche, put each microfiche in a separate paper jacket. If needed, add shredded or crumpled paper before burning. When burning floppy disks, remove the disk from its casing.

2. Use acetone or methylene chloride to destroy microfiche or microfilm when burning is not feasible. Enclose each in a separate paper jacket or place in the chemical bath one at a time for approximately 5 minutes. **WARNING: Use acetone carefully, it is volatile, toxic, and flammable. Avoid spark or flame and wear gloves, aprons, and eye protection. Consult the applicable Material Safety Data Sheet (MSDS) and local safety officer for additional precautions.**

(c) Destroy magnetic or electronic storage/recording media as follows:

1. Destroy magnetic tapes through degaussing or burning. Magnetic cores must be destroyed through burning or smelting. Destroy magnetic disks and disc packs that have been used to store COMSEC material by removing the entire recording surface by means of an emery wheel or sander. **WARNING: Do NOT burn magnetic tape on aluminum reels in a sodium-nitrate fire (this may cause an explosion).**

2. Floppy diskettes may be destroyed through degaussing, burning, or shredding (after removal of the media from the enclosed casing. Ensure any identifying labels are removed from the media and shredded, burned or disintegrated.

(d) Destruction of keying material onboard surface ships, submarines and aircraft will be performed as indicated in the above sections. When such cannot be complied with due to technical reasons, the keying material must be destroyed by reasonable means such as cutting, shredding, etc… and **the residue retained based on the highest classification until terminal destruction can be affected.** Options consistent with national policy are outlined below.

1. Ships may destroy microfiche, floppy disks, and superseded keying material by cross-cut shredding and streaming the residue material loosely into the wake of the ship in open water no closer than twelve nautical miles when the CO/OIC considers recovery by hostile forces unlikely. If in port, temporarily retain the crosscut shredded material until the ship returns to sea whereby the shredded material can be loosely discarded as described above. Store the shredded material in burn bags within a restricted area/space. Storage in a GSA-approved security container or vault is not required, nor is TPI handling and storage required for such residue.

2. Submarines ***in port*** may destroy microfiche, floppy disks, and superseded key tape using a NSA-approved shredder and retain the residue onboard until return to sea and the next available jettisoning operation. When at-sea, submerged submarines with hydraulic compactors shall compress the shredded material into a standard disposable perforated metal container with a minimum weight of 30 pounds, then jettison no closer than 12 nautical miles from land in accordance with Navy and Submarine regulations.

3. On board aircraft, microfiche, floppy disks, and superseded keymat may be shredded using a crosscut shredder currently in inventory and kept in secure storage until a facility is reached where complete/terminal destruction can be accomplished. In emergency situations, deployed aircrew may stream crosscut shredded material loosely from the aircraft over open waters.

Puncture empty key tape canisters on both sides of the canister and dispose of it as unclassified material. Ensure that the canister is empty before disposing of it.

545. COMSEC FACILITIES:

a. **Introduction**: COMSEC facilities include different types of secure telecommunications facilities and other facilities in which classified COMSEC material is contained.

b. **Types of COMSEC Facilities**:

(1) Fixed.

(2) Special-Purpose which includes:

(a) Unattended fixed secure telecommunications facilities.

(b) Contingency fixed secure telecommunications facilities.

(c) Fixed secure subscriber facilities.

(3) Transportable and Mobile.

(4) DOD Bulk Encryption Facility.

c. **Construction Requirements**: The different types of facilities are grouped into categories and their minimum construction requirements are delineated in Annexes N and O. Maximum physical security is achieved when COMSEC facilities are constructed in accordance with the vault-type construction requirements in Annex N.

550. SAFEGUARDING FIXED COMSEC FACILITIES:

a. **Location**: Locate a fixed COMSEC facility in an area which provides positive control over access, and as far as possible from areas which are difficult or impossible to control (e.g., parking lots, ground floor exterior walls, multiple corridors or driveways, or surrounded by other uncontrolled buildings or offices).

b. **Construction Requirements**: See Annex O. COMSEC Facilities approved by an Accrediting Official in accordance with ICD-705 standards shall be assumed to comply with the standards contained herein and do not require separate facility approval or further inspection by COMSEC personnel.

c. **Installation Criteria**: Facilities that generate, process, or transfer unencrypted classified information by electrical, electronic, electro-mechanical, or optical means shall conform to the guidance and standards herein and OPNAVINST C5510.93 (series) (Navy/Marine Corps Implementation of National Policy on Control of Compromising Emanations).

d. **Facility Approvals, Inspections, and Tests**:

A fixed COMSEC facility that contains classified COMSEC material and is located in an immovable structure or aboard a ship.

Consistent with National Doctrine, a COMSEC facility is not:
An office area where only user-level COMSEC equipment are

available for individual use. Examples of an office area includes, but is not limited to: an area with Secure Terminal Equipment (STE), Secure Voice Over Internet Protocol (SVOIP) or Secure Communications Interoperability Protocol (SCIP) products for individual secure voice conversations, a residence with a SIPRNet connection, a single TACLANE or HAIPE device, or a set of cubicles each with its own user level COMSEC equipment. COMSEC material in office areas must be protected, at a minimum, in a manner affording the protection normally provided to other high value/sensitive material, and ensuring access and accounting integrity is maintained. If classified information is being secured by the COMSEC equipment in the office area, the area must be authorized for use or storage of classified information per guidelines from the local security office.

(1) Approval to hold classified COMSEC material. Each facility must be approved to hold classified COMSEC material prior to its use by a competent security official from the responsible department/agency (Immediate Superior in Command or Type Commander (ISIC/TYCOM)). Under no circumstances will EKMS Managers approve facilities and/or spaces within their own organization. For LEs not assigned to the Local Account command, the LEs ISIC/IUC will conduct the COMSEC facilities approval for that LEs secure space or facility. Such approval should also clearly be defined in any Letters of Agreement (LOAs) used to establish a COMSEC support relationship.

NOTE: Unless prohibited by Local, ISIC or TYCOM policy, when a qualified security official is not available from the ISIC activity, activities may request a security official from another nearby organization or installation perform the facility approval provided the same criteria is used in making the determination as noted in d.1.a below.

(a) This approval should be based upon a physical security inspection that determines whether or not the facility meets the physical safeguarding standards of this chapter and Annex N. Checklists are available in EKMS-3(series) Annex D and E for vaults or Fixed COMSEC Facilities, as applicable.

(b) After initial approval, periodic reinspections will be conducted based on threat, physical modifications, sensitivity of programs and past security performance. Unattended telecommunications facilities will be inspected at approximately 30-day intervals to confirm integrity of the facility; competent U.S. personnel must perform these inspections only.

(c) The facility shall also be reinspected, and approval confirmed, every 24 months as part of the required biennial EKMS inspection, when there is evidence of penetration or tampering, after alterations that significantly change the physical characteristics of the facility, when the facility is relocated, or when it is reoccupied after being temporarily abandoned.

AMD-9

NOTE: If necessary, consult with the Physical Security Officer, Security Manager, EKMS Manager or ~~CMS A&A Training~~ COR Audit Team for advice about ~~inspections~~ audits.

(2) Approval to Operate Secure Telecommunications Facilities and Key Distribution Centers:

(a) General COMSEC Inspection. In addition to the physical security inspection above, a general COMSEC inspection must be conducted prior to initial activation, where practicable, but in no case later than 90 days after activation. Thereafter, facilities must be reinspected based on threat, physical modifications, sensitivity of programs, and past security performances. At a minimum, the inspection must address secure operating procedures and practice handling and storage of COMSEC material and routine and emergency destruction capabilities.

(b) Technical Security Evaluation (TSE). All reasonable countermeasures must be taken to ensure that there are no clandestine surveillance devices in COMSEC facilities. Evaluations for clandestine surveillance devices must be conducted as appropriate to the threat level determined by the cognizant security office. TSEs must be conducted when facilities are initially activated or reactivated after foreign occupation, or when there is known or suspected access by foreign maintenance or construction personnel, or when clandestine surveillance or recording devices are suspected in or near a COMSEC facility.

(3) Daily Security Check:

(a) In a continuously manned facility, a security check will be conducted at least once every 24 hours to ensure that all classified COMSEC information is properly safeguarded, and that physical security protection system/devices (e.g., door locks and vent covers) are functioning properly.

(b) 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).

(c) If a facility is in an area posing a high risk of capture by an adversary and the 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.

(4) Quadrant Inspections. A quadrant inspection is designed to detect attempts at technical exploitation of COMSEC equipment by tampering, bugging, key extraction, or reverse engineering. If any of these conditions are known or believed to have taken place, contact NCMS//N5// for additional guidance.

NOTE: Document miscellaneous inspections (e.g., daily security checks, security check after reoccupying a building that was abandoned temporarily) locally in accordance with command directives.

e. **Access Restrictions and Controls**:

(1) Escorted and Unescorted Access:

(a) Limit unescorted access to individuals whose duties require such access, and who meet the access requirements of Article 505 and 535.

(b) Enter the names of persons having regular duty assignments in the facility on a formal access list.

(c) The responsible authority may grant access to cleared and uncleared visitors provided they require such access. Uncleared visitors must be continuously escorted by a properly cleared person whose name is on the access list. Additionally, the space should be sanitized (no classified material left in plain view) when permitting uncleared personnel access.

NOTE: When uncleared 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.

(d) Record all visits in the visitor register and retain the register for at least one year after the date of the last entry. 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) Purpose of visit.
(4) Signature of authorized individual admitting the visitor(s).

(2) No-Lone Zone (NLZ). Area that, when staffed, must be occupied by two or more appropriately cleared individuals who must remain within sight of each other.

(a) Facilities that produce or generate key (e.g., key distribution centers) shall employ NLZ restrictions within all areas in which these activities take place.

(b) Facilities charged with providing or supporting essential, critical, intelligence, or command and control activities should also implement NLZ restrictions.

(c) In addition, departments and agencies may require NLZ restrictions in facilities engaged in the design, development, manufacture or maintenance of crypto equipment.

(3) Firearms. The CO or responsible civilian official shall determine the need for firearms to protect a facility as stated in department and agency directives.

f. **Storage of COMSEC Material**: Store COMSEC material in accordance with Articles 520 and 535.

g. **Protection of Unattended COMSEC Equipment**:

(1) In a non-continuously manned facility, protect unattended COMSEC equipment in accordance with Article 520 and/or 535 during periods when the facility is not manned.

(2) A facility that meets the construction requirements of Annex O provides sufficient protection, under normal circumstances, for unattended, unkeyed COMSEC equipment

installed in an operational configuration.

NOTE: Requirements for the protection of COMSEC equipment in facilities that normally operate unmanned for extended periods of time are delineated in Article 555.

h. **Protection of Lock Combinations**: The requirements for protection of lock combinations to security containers in Article 515 applies to all COMSEC facility doors.

i. **Standard Operating Procedures (SOPs)**: Each facility shall have a written SOP. Ensure the SOP contains provisions for securely conducting facility operations and for safeguarding COMSEC material. Additionally, each facility shall have an Emergency Protection Plan in accordance with Annex M.

j. **Non-essential Audio/Visual Equipment**:

(1) Personally-owned receiving, transmitting, recording, amplifying, information-processing, and photographic equipment (e.g., tape recorders, stereos, televisions (with VCR capabilities), cameras, cellular phones, laptop computers, workstations, web based phones, two-way pagers, portable music players with memory (iPods), magnetic tape and film) shall not be permitted in secure telecommunications facilities or key distribution centers. Radios are permitted providing that the device does not have record capabilities or the record/playback capability is disabled.

(2) Government-owned or leased, or company-owned or leased in the case of contractor-operated facilities, receiving, transmitting, recording, amplifying, video, and photographic equipment (e.g., cellular phones radios, music systems, TV monitors/cameras, and amplifiers) which are not directly associated with secure telecommunications operations or information processing activities are prohibited in COMSEC facilities unless approved in writing by the Commanding Officer for conduct of official duties, and must meet the requirements of OPNAVINST C5510.93 (series).

(3) Personal Electronic Devices (PEDs)/Personal Digital Assistants (PDAs): As the capabilities of these devices increase, the potential risk from using them in or around areas where classified information may be discussed or processed also increases. NSA continues to recommend extreme caution in allowing the introduction of any PED/PDA (whether it uses wireless applications or not) within secure spaces where

classified information may be stored, processed, or discussed. Before local authorities approve the introduction of such devices; it is recommended that managers and users be made fully aware of associated risks. All current facility restrictions (e.g., no Infrared (IR)/Radio Frequency (RF) transmitters) should be followed to ensure the entry of PEDs/PDAs does not violate technical security policies. At a minimum, PEDs/PDAs should be turned off, with the batteries removed, when being brought into these locations. Malicious code by an adversary or even some vendor applications can turn the transceiver back on without the user's knowledge.

(4) Microphones

(5) Nothing in this publication shall be construed to contradict or inhibit compliance with the law, such as the Americans with Disabilities Act, building codes, federal antiterrorism standards, or other applicable statues.

555. SAFEGUARDING UNATTENDED FIXED SECURE TELECOMMUNICATIONS FACILITIES:

An unattended fixed secure telecommunications facility is an operational facility in which secure telecommunications functions are performed with no operator personnel present. Such a facility normally, but not exclusively, performs a communications relay or other similar switching function. The following particulars are applicable:

a. **Location**: Locate these facilities in areas firmly under U.S. or Allied control, where sufficient U.S. or Allied military or police forces are located in the vicinity to provide reasonable protection against unauthorized occupation of the site.

b. **Construction Requirements**: Construct these facilities in accordance with Annex O. Primary entrance doors shall be limited to one. Windows less than 18 feet above the ground, measured from bottom of the window, or are easily accessible by means of objects directly beneath that window, will be covered by an IDS.

c. **Installation Criteria**: Comply with guidance in Article 550.c.

d. **Facility Approvals, Inspections, and Tests**: In addition to the guidance listed in Article 550, inspect unattended facilities at approximately 30-day intervals to confirm the integrity of the facility.

e. **Access Restrictions and Controls**: Article 550.e. applies. Additionally, all persons who visit the facility, including those on the official access list, shall record each visit in the visitor register.

(1) Protect each facility with an approved IDS which provides for an on-the-scene guard response within fifteen minutes or protect it with guard(s).

(2) If the guard response to an alarm will be more than 15 minutes, select crypto equipment for use at the facility that employs a system for remote zeroization.

f. **Storage and Protection of COMSEC Material**:

(1) Only operational crypto equipment and currently effective key held in that equipment shall be permitted at an unattended facility.

(2) Do not store future key (ROB), non-operational or spare crypto equipment, or COMSEC publications (e.g., maintenance manuals or operating instructions).

(3) Install operational crypto equipment in NSA-approved containers, or use supplementary controls (e.g., locking bars secured with a changeable combination lock meeting FF-P-110J, FF-L-2740 or FF-L-2740A specifications or an approved IDS).

NOTE: 1. DIRNSA-approved security containers for operational crypto equipment may not be procured after 30 June 1999. These containers may continue to be used to store keyed on-line COMSEC equipment that supports nets/circuits terminated in spaces that are not continuously manned by appropriately cleared people, provided no computer data files are stored with the COMSEC equipment. These containers are not approved by GSA because they have holes drilled in them for signal, power, and cooling.

2. GSA-approved Class 5 Information Processing System (IPS) containers that have been drilled for signal, power, and cooling may be used to store keyed on-line COMSEC equipment that supports nets/circuits terminated in spaces that are not continuously manned by

appropriately cleared people.

g. **Protection of Lock Combinations**: Protect combinations in accordance with Article 515. Additionally, do not store records of lock combinations at an unattended facility.

h. **Firearms**: Article 550.e.(3) applies for guards or for other personnel who may visit the facility.

i. **Standard Operating Procedures (SOP)**: See Article 550.i.

j. **Non-essential Audio/Visual Equipment**: Comply with Article 550.j.

k. **Additional Security Requirements**: Personnel who visit an unattended facility to key the equipment or perform maintenance, must inspect the facility for signs of tampering or attempted penetration.

560. SAFEGUARDING CONTINGENCY FIXED SECURE TELECOMMUNICATIONS FACILITIES:

a. **General**:

(1) These facilities contain secure telecommunications equipment in an operational configuration for rapid activation as a fully operational facility should the need arise.

(2) They may be fully equipped, or they may be partially equipped and made ready for secure communications at the time of activation.

(3) They are normally unattended, or are attended only on a part-time basis.

b. **Location**: Article 550.a. applies.

c. **Construction Requirements**: Annex O applies.

d. **Installation Criteria**: Article 550.c. applies.

e. **Facility Approvals, Inspections, and Tests**: Article 550.d applies; inspect these facilities at approximately 30-day intervals to confirm the integrity of the facility and to remove any superseded or extraneous material.

f. **Access Restrictions and Controls**: Article 550 applies;

these facilities shall have either an approved IDS or shall be guarded.

g. **Storage of COMSEC Material**: Store COMSEC material in accordance with Article 520 and/or 535.

h. **Protection of COMSEC Equipment**: Where the facility is not contained in a vault constructed as specified in Annex N, install all crypto equipment in DIRNSA-approved security containers for storage of operational crypto equipment, or use supplementary controls (e.g., locking bars to secure the equipment or an approved IDS).

i. **Protection of Lock Combinations**: Protect lock combinations in accordance with Article 515. Additionally, do not store records of lock combinations at unattended contingency facilities.

j. **Firearms**: Article 550.e.(3) applies.

k. **Standard Operating Procedure (SOP)**: Article 550.i applies.

l. **Non-essential Audio/Visual Equipment**: Article 550.j applies.

m. **Additional Security Requirements**: Personnel who visit a contingency facility during periods when it is unattended shall inspect the facility for signs of tampering or attempted penetration.

565. SAFEGUARDING FIXED SECURE SUBSCRIBER TELECOMMUNICATIONS FACILITIES:

a. **General**:

(1) A fixed secure subscriber telecommunications facility is a structure, or area within a structure, in which user-operated secure voice, data, facsimile, or video circuits terminate. **An office in which a STE is installed is not a Secure Subscriber Telecommunications Facility.**

(2) Although these facilities are often inherently difficult to control, sufficient controls must be provided to prevent unauthorized persons from using the terminal equipment and to protect the associated crypto equipment and keying material.

Note: Storage of classified material in a private residence or residential SIPRNET installation must be approved in advance of the storage or installation, as applicable in accordance with NTD 03-09, SECNAV M5510.36 Article 10-10 or per service-specific regulations and ODAA guidance (USMC/USCG). If approved, a GSA-approved security container secured to the building structure and equipped with a FF-L-2740/2740A combination lock is required.

b. **Location**: See Article 550. Additionally, locate the facility within the building proper (i.e., not on balconies, porches, bays, or other architectural projections that are not of substantial construction). Also, locate the terminal equipment in an area away from heavy pedestrian traffic.

c. **Construction Requirements**: A fixed secure subscriber facility ideally should be located in an area conforming to the construction requirements of Annex O. Where this is not practicable (i.e., general office spaces and residences), rigidly apply the applicable requirements which follow.

d. **Access Restrictions and Controls**: Limit unescorted access to the crypto equipment and associated COMSEC material to individuals who require such access and who meet the access requirements of Article 505 and/or 535.

(1) Limit unescorted use of the terminal equipment for secure communications to appropriately cleared individuals.

(2) Uncleared individuals, or persons not appropriately cleared, may use the terminal equipment for secure communications provided they are escorted by an individual who has unescorted access, and the distant end is first notified of the clearance limitations.

(3) In general office environments and in private residences where individuals work, reside, or visit, take precautions to ensure that unauthorized persons do not overhear classified conversations and that classified messages are not left unattended.

e. **Storage of COMSEC Material**: Store COMSEC material in accordance with Article 520 and/or 535. Facilities other than those in private residences may hold only the current edition of keying material and operating instructions for the crypto equipment, but no other supporting COMSEC material.

(1) Facilities in private residences may hold no more than a seven-day supply of keying material (except where the key is either packaged in a protective canister or issued to a DTD; then, the current edition may be held).

(2) Facilities in private residences may hold no other supporting COMSEC material.

f. **Protection of Unattended COMSEC Equipment**: Protect unattended crypto equipment to a degree, which, in the judgment of the responsible official, is sufficient to preclude any reasonable chance of pilferage, theft, sabotage, tampering, or access by unauthorized personnel.

(1) When possible, install the crypto equipment in a NSA-approved security container for storage of operational crypto equipment. Alternatively, protect the equipment by an approved IDS, or by a security force.

(2) Whenever the facility is vacated by all appropriately cleared personnel, unkey the equipment and securely store the keying material.

(3) For facilities in private residences and other unprotected areas or facilities (when the user is absent for a period of more than 72 hours), remove and securely store all classified components of the system.

570. SAFEGUARDING TRANSPORTABLE AND MOBILE COMSEC FACILITIES:

a. **General**: The safeguards contained in this Article are primarily applicable to transportable and mobile secure telecommunications facilities, but they also apply to any other transportable or mobile facility that contains classified COMSEC material (e.g., a transportable crypto-maintenance facility or a transportable or mobile key distribution center (KDC)).

b. **Location**: These facilities may be located wherever operational requirements dictate.

c. **Construction Requirements**: Construction requirements are not prescribed for these facilities because of the many possible operational requirements that such facilities must fulfill.

d. **Installation Criteria**: Article 550.c. applies.

e. **Facility Approvals, Inspections, and Tests**:

(1) Approval as stated in Article 550 is generally not required. The only inspection requirement is for a daily security check.

(2) After remaining in a fixed position for a period of three months or longer, transportable or mobile facilities should normally be considered as fixed facilities. Consequently, a facility approval, inspection, and test must be conducted in accordance with Article 550.

(3) If a transportable or mobile facility processes especially sensitive information or frequently operates where a known hostile intelligence threat exists, the requirements for TEMPEST inspections apply.

f. **Access Restrictions**: Article 505 and/or 535 applies, except on-duty uncleared crewmembers (e.g., in aircraft and tanks) do not require a continuous escort by an individual who has unescorted access.

NOTE: Transportable and mobile facilities employed primarily to perform telecommunications or key distribution functions (e.g., a communications van or mobile KDC) shall maintain both access lists and visitor registers.

g. **Storage of COMSEC Material**: Store COMSEC material in accordance with Article 520 and/or 535 and comply with the following additional requirements:

(1) Securely affix security containers to the facility with bolts, welds, or other appropriate means.

(2) Limit COMSEC material holdings to those operationally necessary to fulfill mission requirements (i.e., normally a single edition). Do not hold full maintenance manuals.

h. **Protection of Unattended Facilities**:

(1) Secure and guard facilities whenever they are left unattended. Because of the many structural variations in these facilities (e.g., vans, aircraft, and open vehicles), standardized criteria for securing them cannot reasonably be prescribed.

(a) Where a facility is inside a solid enclosure (e.g., van or equipment shelter), secure all access points (e.g., windows) from inside, and secure the entrance door with an electro-mechanical lock meeting Federal Specification FF-L-2740/2740A requirements.

(b) Where this is not practicable (e.g., open vehicle or aircraft), use an approved locking bar or other locking device to prevent tampering or removal of the crypto equipment.

(2) Guard unattended transportable and mobile COMSEC facilities as follows:

(a) Use U.S. guards when the facility contains keying material or keyed crypto equipment.

(b) A roving guard(s) making rounds at least every four hours is sufficient protection for facilities located in U.S. or Allied territory.

(c) U.S. guards must be used (and they must be in the immediate area of the facility at all times) for facilities located in non-U.S. or non-Allied territory.

i. **Protection of Lock Combinations**: Article 515 applies.

j. **Firearms**: Article 550.e.(3) applies.

k. **Standard Operating Procedure (SOP)**: Article 550 applies to transportable, but not to mobile COMSEC Facilities.

575. SAFEGUARDING DOD BULK ENCRYPTION FACILITIES:

a. **General**: Bulk encryption facilities operated by or for the DOD, and employ classified crypto equipment to protect multi-channel trunks passing national security-related information. A bulk encryption facility consists of multi-channel terminal(s) and associated crypto equipment.

b. **Definitions**:

(1) A space is the area within a structure occupied by a DOD bulk encryption facility. A space may be integrated into an area containing other communications equipment, or it may be a room or enclosure dedicated to the multi-channel terminal(s) and associated crypto equipment only.

(2) A site is the structure that contains a space.

(3) Appropriately Cleared means possessing a CONFIDENTIAL or higher security clearance issued by the U.S. Government, or an equivalent clearance issued by a foreign government or an international organization to which the crypto equipment has been released.

c. **Safeguarding Criteria**: Because of the unique nature of bulk encryption facilities, they may be operated in many different environments and under varying degrees of security risk. Some requirements are the same as for normal fixed facilities, others are not.

d. **General Requirements**:

(1) Installation Requirements. Whenever possible, installations should conform to the installation RED/BLACK criteria. The appropriate department or agency authority shall determine the requirement for application of this criteria on a case-by-case basis.

(2) Facility Approvals, Inspections, and Tests. The provisions of Article 550.d. are applicable. However, TSCM inspections and instrumented TEMPEST tests are not required.

(3) The protection of lock combinations; a determination for the need of firearms; maintaining an SOP; and the use of nonessential audio/visual equipment are delineated in Article 550.j.

e. **Special Requirements**: Annex P contains special requirements for physical security safeguards for DOD bulk encryption facilities and safeguarding COMSEC material used therein.

CHAPTER 6 -- MAINTAINING COMSEC MATERIAL ALLOWANCE

CHAPTER 6 - MAINTAINING/MODIFYING A COMSEC MATERIAL ALLOWANCE

601. GENERAL:

a. CMIO Norfolk acting on behalf of NCMS, manages the authorized allowance of COMSEC material as validated by the ISIC of the command.

b. The EKMS account number (e.g., CA141126) must be reflected on all messages pertaining to the accounts authorized allowance.

c. After ISIC validation of a command's authorized allowance, physical COMSEC material is initially distributed via an authorized courier (e.g., Defense Courier Service (DCS), or issued directly to a Manager via over-the-counter (OTC) pickup at a Vault, Depot, and Logistic System (VDLS) component).

d. Keying material may also be generated in electronic form (i.e., traditional 128-bit key) by Tier 0, Tier 1, or locally by a Tier 2 using a KP or other key variable generator and distributed physically in a fill device (FD) or transmitted electronically via a telecommunications circuit.

e. The authorized COMSEC material allowance for each command is based on its assigned mission and communications capabilities.

602. COMMON ACCOUNT DATA (CAD):

a. The CAD is the primary means used by the COR to determine Point Of Contact Information for EKMS Accounts. Failure to maintain accurate and up-to-date CAD data could result in:

(1) Failure to receive electronic key

(2) Delays in receiving physical keymat or COMSEC equipment as a result of an incorrect shipping address.

AMD-9 (3) Delays in obtaining assistance from NCMS, ~~A/A Teams~~ COR Audit Teams, the EKMS Technical Support Center or other agencies due to incorrect contact information. e.g. phone numbers, email addresses, etc.

b. EKMS Managers must frequently review and update their

CAD, and ensure the following information is correct:

(1) The names of the EKMS Manager and Alternates.

Submarine accounts with Blue and Gold crews only: In the Primary Manager Field: The present manager of the active crew preceded by the first letter of the active crew, i.e., G ITCS Longfellow. In the Alternate Manager Fields: First line will be the Primary Manager of the inactive crew followed by **all** Alternates preceded by the first letter of the crew, i.e., B Ens. Jones; G Ens. Smith.

(2) Primary and Alternate phone numbers where the EKMS Manager/Alternate can be reached. If Duty Officer numbers are provided, ensure the Duty Officers are provided POC information for the Account Managers.

(3) Mailing Address: Outer wrapper information.

(4) NIPRNET and SIPRNET email addresses for the EKMS Manager and Alternates.

Submarine accounts with Blue and Gold crews only: Enter only the SIPRNET email address for each alternate preceded by the first letter of the crew, i.e., Bjonesj(at)ohio.navy.smil.mil; G smithj(at)ohio.navy.smil.mil. If sufficient room is not available to enter the email address for all alternates, then enter only one alternate per crew. If the SIPRNET and NIPRNET email addresses are the same with the exception of ".smil" then enter as: Bjonesj(at)ohio.navy(.smil).mil.

(5) Name, rank/grade and NIPRNET and SIPRNET address of the Commanding Officer. (This data will be maintained and updated in one of the blank Alternate Manager fields.

Submarine accounts with Blue and Gold crews only: For COs: Will reflect only the name/rank preceded by the first letter of the crew, i.e., B CAPT. Johnson; G CAPT. Marks(or use CDR, as applicable in lieu of CAPT).

NOTES: (1) CAD data will be reviewed and updated at a minimum of semi-annually in conjunction with the SAIR inventory, when a Change of EKMS Manager or Change of Command inventory is conducted and when a change in EKMS Manager or Primary Alternate occurs. In doing so, phone numbers, email addresses, etc… should also be verified and updated, as applicable.

(2) USMC Accounts may use either the name of the Commanding Officer or ISIC, as desired in meeting the requirement noted in paragraph 602.b.5 above.

605. COMSEC EQUIPMENT, RELATED DEVICES, EQUIPMENT MANUALS AND OPERATING INSTRUCTIONS ALLOWANCE. An account allowance for COMSEC equipment, related devices, equipment manuals and operating instructions is based upon an approved allowance list in accordance with the following guidelines and/or authorities:

a. **Navy, Coast Guard, and MSC Commands**:

(1) The type and quantity of cryptographic equipment and related devices that a command is authorized to hold is contained in the NAVY CONSOLIDATED SECURE VOICE AND RECORD PLAN as validated by the CNO and maintained by SPAWARSYSCEN ATLANTIC Charleston, SC.

(2) Shipboard allowances by ship type and/or design are based, in part, upon the guidance contained in OPNAVINST 2300.44 (series).

(3) ISICs may provide additional guidance as required.

b. **USMC Commands**:

NOTES: 1. Procedures herein for "USMC Commands" are only applicable to those Marine Corps organizations whose COMSEC equipment is authorized by and established in a Table of Equipment (T/E) and that COMSEC equipment is in support of "Green Dollar" Marine Corps T/E equipment.

2. Marine aviation organizations whose COMSEC equipment is not authorized by and established in a T/E and is in direct support of "Blue Dollar" Navy (Non-T/E systems and aircraft) must follow procedures delineated for "Navy Commands".

AMD-9

(1) As published in individual unit's T/E and/or guidance promulgated by Commandant, Marine Corps//C4/C4 CY//, Commander, CMC C FOUR CY Washington DC~~//C4/C4 CY~~// and/or CG MARCORLOGCOM Albany GA.

AMD-9

(2) Under the authority of CMC C FOUR CY Washington DC~~//C4/C4 CY~~//, the following commands will transfer COMSEC equipment and related devices between USMC accounts only:

COMMARCORSYSCOM Quantico VA//CINS// and/or CG MARCORLOGCOM Albany GA.

(3) The procedures for modifying allowances of COMSEC equipment and related devices, on a routine and emergency basis that are detailed in Article 655 and 675, respectively, are **not** applicable to USMC commands subordinate to COMMARFORCOM/PAC/RES, and CGs at the Marine Expeditionary Force (MEF), Marine Division (DIV), Marine Aircraft Wing (MAW), and Marine Logistic Group (MLG) levels.

(4) CMC C FOUR CY WASHINGTON DC// and USMC Commanders cited above are authorized to manage the USMC COMSEC equipment and related devices in the EKMS accounts of subordinate USMC units.

(a) Temporary transfers, not to exceed eight months, will be accomplished on a local custody basis.

(b) Permanent transfers, in excess of eight months, will be conducted via an SF-153 account-to-account transfer report.

NOTE: CMC C FOUR CY WASHINGTON DC//, COMMARCORSYSCOM QUANTICO VA//CINS//, CG MARCORLOGCOM ALBANY GA, NCMS//N3//, and the Chain of Command must be information addressees on all correspondence directing the permanent transfer of equipment and related devices.

610. VALIDATION OF CRYPTOGRAPHIC EQUIPMENT AND RELATED DEVICES:

a. CNO validation and approval is required for all cryptographic equipment and associated ancillary devices. Further guidance related to equipment allowances, transfers, recertification, etc… can be found in EKMS-5(series).

b. Submit requests for review, validation, and approval in the following format:

(1) Navy and MSC Commands:

TO: COMUSFLTFORCOM NORFOLK VA//N023EKMS//
or
COMPACFLT PEARL HARBOR HI//N633//

INFO: CNO WASHINGTON DC//N2/N6F1133//

ISIC
Administrative Chain-of-Command
NCMS WASHINGTON DC//N3//
CMIO NORFOLK VA//N3/N35//

NOTE: Corresponding COMFLTs will coordinate directly with CNO for the validation request.

(2) Coast Guard Commands:

TO: COGARD C4ITSC ALEXANDRIA VA
INFO: CNO WASHINGTON DC//N2/N6F1133//
ISIC
Administrative Chain-of-Command
NCMS WASHINGTON DC//N3//
CMIO NORFOLK VA//N3/N35//

NOTE: COGARD C4ITSC will coordinate directly with CNO for the validation request.

(3) USMC Commands: Per Article 605.b. NOTE 1 (Green Dollar)

TO: CMC C FOUR CY WASHINGTON DC//
INFO: ISIC
Administrative Chain of Command
COMMARCORSYSCOM QUANTICO VA//CINS//
CG MARCORLOGCOM ALBANY GA
CNO WASHINGTON DC//N2/N6F1133//
NCMS WASHINGTON DC//N3//
CMIO NORFOLK VA//N3//N35//

SUBJ: REQUEST FOR CRYPTO EQUIPMENT VALIDATION

(a) Justification for the operational requirement, including the detail that will permit establishment of its relative priority in the general program.

(b) A block diagram of the existing and/or proposed circuit.

(c) The type and general reliability of the transmission medium.

(d) Identification of all terminals on the proposed circuit.

(e) The estimated, average daily volume of classified and unclassified traffic to be handled on the proposed circuit, the maximum classification of that traffic, and any special requirements for such traffic.

(f) Expected use of the proposed circuit.

(g) The nomenclature and quantity of terminal equipment required for the proposed circuit (including an indication of equipment on hand).

(h) Remarks pertinent to compliance with guidance provided by OPNAVINST C5510.93 (series) concerning minimizing compromising emanations or other electromagnetic radiations.

(i) A statement of ability to comply with security criteria, or a description and estimated cost of any modification that may be required.

(j) When landline connections are involved, identify the command that will pay for the telephone lines and/or lease telephone company modems, etc.

(k) A statement that maintenance personnel qualified in accordance with OPNAVINST 2221.3 (series) will be available or that an increase of such personnel will be required to maintain the cryptographic equipment.

(l) Specify the date the material is needed.

(m) EKMS account number.

615. COMSEC KEYING MATERIAL RESERVE-ON-BOARD (ROB):

a. The quantity of future editions of keying material (i.e., reserve-on-board (ROB)) to be held by an EKMS account is determined by the COMFLT, CMC, ISIC, or COGARD C4ITSC.

b. Factors such as operational requirements, type of command (fixed or mobile), location, duration and area of deployment for mobile units, and the resource limitations and/or geographical constraints of the DCS are to be considered when establishing a standard ROB level for an account. ROB levels can range from two to six months of keying material.

620. MAINTAINING ROB LEVELS OF KEYING MATERIAL:

a. Each EKMS account command must ensure that all effective and ROB editions of authorized holdings are maintained and requests for increases or reductions are submitted as operational requirements change.

b. It is the responsibility of each EKMS account to review their holdings on an annual basis to ensure a continuing need for the quantity and types of all COMSEC material held.

c. Mobile accounts must keep DCS and CMIO informed of their movements (e.g., deployments, underway schedule) to ensure timely delivery of their ROB material. As noted in Article 602, EKMS Managers are responsible for keeping their CAD data updated at all times.

d. If the ROB level falls **below two months** of keymat, a message must be sent action to CMIO Norfolk, VA, info NCMS WASHINGTON DC//N3// and COMFLTs indicating the last edition held and requesting assistance in obtaining follow-on editions.

NOTE: Superseded material received in a ROB shipment must be destroyed within 12 hours of opening the shipment. Annotate on the SF-153, "SUPERSEDED UPON RECEIPT." No additional reporting is required.

e. If necessary, contact NCMS N3 Key Division and CMIO Norfolk via message to request re-supply of COMSEC material to maintain ROB for any reason, i.e., receipt of damaged material that DIRNSA provides disposition for (return of material to DIRNSA or authorized destruction), inadvertent or early destruction, EAP implemented destruction, or lost/missing ROB material.

f. Modern FIREFLY key is not automatically resupplied. EKMS Managers **must** review and track associated production dates and submit key orders to the EKMS CF prior to the 1 year expiration date for this type of material.

NOTE: Depending on the situation, the reporting requirements stated in Articles 1005 and 1010 may apply.

g. ROB stock level table for electronic and physical (**use as a general guide**):

SUPERSESSION PERIODICITY/QUANTITY TO BE HELD

ROB LEVEL	Yearly	Semi-annual	Qtrly	Bi-monthly	Monthly	15days	10days	7days
2	1	1	2	2	2	4	6	10
3	1	2	2	3	3	6	9	15
4	1	2	2	3	4	8	12	20
5	1	2	2	4	5	10	15	25
6	1	2	3	4	6	12	18	30

h. ROB quantities are in addition to the effective edition being used. The above table can be used as a **general guide** to determine how many editions of keying material are to be held as ROB. Three months of ROB is standard for most EKMS accounts, however, some COMFLT/TYCOM identified units are authorized to hold seven months of material to support extended operations.

625. MODIFYING ROB LEVELS FOR PREVIOUSLY VALIDATED KEYING MATERIAL:

a. A request to increase ROB levels for Short Titles the account is validated for requires at least 60 days notice if material is shipped via DCS. A request to decrease a ROB level requires a minimum of 14 days notice. For material the account has not been validated for, such much be approved by the CONAUTH as discussed in Article 650.

b. Address a request to modify a ROB level as follows:

(1) Navy (see NOTE below), MSC, and USMC supporting establishments:

TO: ISIC
INFO: CMC C FOUR CY WASHINGTON DC//
(USMC commands only)
Chain of Command
CMIO NORFOLK VA//N3//
NCMS WASHINGTON DC//N3//
DIRNSA FT GEORGE G MEADE MD

NOTES: (1) USN surface accounts subordinate to a COMFLT will address their request as reflected below:

(2) SUBFOR/SUBPAC will be INFO Addee on all ROB level changes pertaining to submarines.

TO: COMPACFLT PEARL HARBOR HI//N633// or
COMUSFLTFORCOM NORFOLK VA//N023EKMS//
INFO: ISIC
Chain of Command
CMIO NORFOLK VA//N3//
NCMS WASHINGTON DC//N3//
DIRNSA FT GEORGE G MEADE MD

(2) Coast Guard Commands:

ACTION: COGARD C4ITSC ALEXANDRIA VA//BOD-IAB//
INFO: Area and/or District Commander
Chain of Command
CMIO NORFOLK VA//N3//
NCMS WASHINGTON DC//N3//
DIRNSA FT GEORGE G MEADE MD

(3) Marine Corps Fleet Marine Force (FMF) Commands:

ACTION: COMMARFORCOM, PAC OR RES (See NOTE below)
INFO: CMC C FOUR CY WASHINGTON DC//
Chain of Command
NCMS WASHINGTON DC//N3//
CMIO NORFOLK VA//N3//
DIRNSA FT GEORGE G MEADE MD

c. Provide the following information, in sequence, to modify a ROB level:

Subject: ROB LEVEL CHANGE

(1) EKMS account number and HCI.
(2) Current ROB level.
(3) New level.
(4) Date material required in YYMM format.
(5) Servicing DCS; indicate any special shipping instructions.
(6) Justification.

NOTE: Marine Corps commands must include COMMARFORCOM//G-6// on all such messages.

d. Action addressees must approve, disapprove or modify a request to change a ROB level for subordinates by sending a message to CMIO NORFOLK VA, info NCMS//N3// and the remaining addressees on the original request and the CONAUTH of the keying material.

630. **DEFENSE COURIER SERVICE (DCS)**:

a. The United States Transportation Command, Defense Courier Division (USTRANSCOM TCJ3-C) operates a network of 18 stations to provide the secure, timely and efficient global distribution of classified and sensitive material for the U.S. Government and its allies. The DCS contact website is http://www.transcom.mil/dcd/.

b. Defense Courier Service operates on a reimbursable basis. NCMS and other courier service customers who ship material are charged for the movement based on a fixed rate per pound. The rate is established at the beginning of each fiscal year and remains fixed for the entire year.

c. Mobile units, exercise planners, and major staff commands requesting allowance changes must allow sufficient time in their notification to NCMS and CMIO to allow maximum use of the regularly scheduled missions.

d. Material eligible for shipment via DCS is assigned one of two priorities in the DCS Movement System as follows:

(1) **Regular Movement**: This material, representing the bulk of the material entered into the DCS, moves in accordance with regularly scheduled DCS missions. The majority of COMSEC material is transported via this method.

(2) **Special Movement**: This material is expeditiously moved at the **expense of the requesting command** to satisfy deadlines that cannot be met by regularly scheduled DCS missions. Special movement replaced the former DDD (deadline delivery date) and is normally moved via commercial means based on validated customer needs and available DCS resources.

(a) Commands requesting a special movement must provide a fund site in the request for material and include HQ DEFCOURIERSVC FT GEORGE G MEADE MD//DO// as an ACTION addee. The COR and NCMS//N3// will coordinate special movements between the requesting command and HQ DCS.

(b) Requests for Special movements will be processed and entered into the DCS system within 48 hours or less.

(c) A request for Special movement **without** a fund site will be transported as a "Regular" shipment regardless of the date the material is required.

(d) Accounts are responsible for ensuring DCS is kept informed of their geographical location at all times to prevent delays in delivery of material. Unless prior authorization is received from NCMS, accounts will pick up any material shipped to them through DCS.

> **NOTE: Regardless of grade or position, personnel picking up material from DCS must be authorized by the current CO/OIC of the account as reflected on the Form-10 on file with the servicing DCS station.**

635. DCS ADDRESS CHANGE

a. United States National Distribution Authority (USNDA) processes and automatically ships ROB material to the DCS delivery address of record for an account (as assigned during the DCS account establishment process) 45-60 days prior to receipt by an account.

b. To preclude delays in receipt of material, EKMS accounts must notify NCMS//N3//, info CMIO NORFOLK, the servicing DCS station, and DIRNSA FT GEORGE G MEADE MD whenever there is a change in the servicing DCS station or a change in the command address. When there is a change, both the old and new servicing DCS station must be informed of the new address.

640. OVER-THE-COUNTER (OTC) PICKUP FROM CMIO NORFOLK, A CRYPTO REPAIR FACILITY (CRF) AND THE UNITED STATES NATIONAL DISTRIBUTION AUTHORITY (USNDA):

a. CMIO provides over-the-counter (OTC) pickup of COMSEC equipment for EKMS accounts that do not receive their material via the DCS. USNDA provides emergency OTC pickup when EKMS accounts do not receive their keying material.

b. **ONLY** those commands that will pick up COMSEC equipment directly from the CMIO are required to have an up-to-date CMS Form 1 on file at the CMIO. The CMS Form 1 reflects EKMS Managers and Alternates that are authorized to receipt for and courier COMSEC material between their command and the CMIO. Annex H contains a sample CMS Form 1 and instructions. A sample USTC Form 10 can be found in Annex I.

c. Pickup of COMSEC material from the CMIO is not authorized unless the CMS Form 1 is signed by the current Commanding Officer and updated at a minimum of annually. There are **NO EXCEPTIONS** to this policy.

d. Personnel picking up COMSEC material must carry proper identification and courier authorization.

e. COMSEC material picked up/dropped off from CMIO, a CRF, DCS, or USNDA must be transported directly to/from the command and be properly safeguarded at all times until properly stored or signed for when material is turned in. Delays or stops, except for emergencies, between the command and CMIO, a CRF, DCS or the USNDA, is **strictly prohibited**.

f. EKMS accounts must contact CMIO NORFOLK and info NCMS//N3// via message. CMIO will coordinate with the NSA Duty Officer, to arrange emergency OTC pickup at USNDA.

645. TERMINATION & RESUMPTION OF AUTOMATIC DISTRIBUTION OF COMSEC MATERIAL:

a. Options are available for maintaining EKMS during scheduled overhaul periods or extended periods outside of normal DCS schedules or delivery locations. To preclude potential problems ensuring timely receipt of material for short-notice requirements or schedule changes, it is highly recommended that accounts not terminate their distribution when the overhaul/availability period is less than eight months in duration.

(1). Continue business as usual. The account will continue to receive physical and electronic shipments and be responsible for all accounting functions (e.g. receipts, destruction, and inventory).

(2). Termination of automatic distribution. Accounts can request via message to their ISIC to terminate automatic distribution. Upon concurrence from the ISIC, NCMS will place the account in an “inactive” status in Common Tier 1. Accounts in an “inactive” status will not receive physical or electronic shipments of COMSEC material. Accounts will remain responsible for all accounting functions (e.g., destruction and inventory) for all COMSEC key and equipment that remain on their Accountable Items Summary (AIS). Accounts must ensure that they have a sufficient quantity of key to last through the period they are requesting termination of automated distribution.

(a) Address a request to terminate automatic distribution as follows:

(b) Navy, MSC, and USMC supporting establishments:

TO: ISIC
INFO: CMC C FOUR CY WASHINGTON DC//
Chain of Command
CMIO NORFOLK VA//N3//
NCMS WASHINGTON DC//N3//
DIR TIER1 SAN ANTONIO TX or
CSLA TIER1

(c) USN surface accounts subordinate to a COMFLT will address their request as follows:

TO: COMPACFLT PEARL HARBOR HI//N633// (PACFLT SHIPS) or
COMUSFLTFORCOM NORFOLK VA//N023EKMS// (LANTFLT SHIPS)
INFO: Chain of Command
CMIO NORFOLK VA
NCMS WASHINGTON DC
DIR TIER1 SAN ANTONIO TX or
CSLA TIER1

(d) Submarine accounts will address their request as follows:

TO: COMSUBPAC PEARL HARBOR HI (for PACFLT Submarines)
or
COMSUBFOR NORFOLK VA (for LANT submarines)
INFO: Chain of Command
CMIO NORFOLK VA
NCMS WASHINGTON DC
DIR TIER1 SAN ANTONIO TX or
CSLA TIER1

(e) Coast Guard accounts will address their request as follows:

TO: COGARD C4ITSC ALEXANDRIA VA//BOD-IAB//
INFO: Area and/or District Commander
Chain of Command

CMIO NORFOLK VA
NCMS WASHINGTON DC
DIR TIER1 SAN ANTONIO TX or
CSLA TIER1

(f) Marine Corp accounts will address their request as follows:

TO: Next Senior Flag Level Command
INFO: CMC C FOUR CY WASHINGTON DC//
Chain of Command
CMIO NORFOLK VA
NCMS WASHINGTON DC
DIR TIER1 SAN ANTONIO TX or
CSLA TIER1

MSGID/GENADMIN/USS UNDERWAY/-/-//
SUBJ/REQUEST TO STOP AUTOMATIC DISTRIBUTION OF COMSEC MATERIAL FOR ACCOUNT NAME (ACCOUNT NUMBER)//
REF/A/DOC/NCMS WASH DC/-/-//
AMPN/REF A IS EKMS-1(SERIES).
RMKS/1. IAW REF A, REQUEST ISIC VALIDATION OF REQUEST TO STOP AUTOMATIC DISTRIBUTION OF COMSEC MATERIAL FOR ACCOUNT NAME (ACCOUNT NUMBER).

A. ACCOUNT NAME:
B. ACCOUNT NUMBER:
C. HCI:
D. EFFECTIVE DATES:
E. REASON FOR REQUEST:
F. SERVICING DCS STATION:
G. REMARKS:

(g) ISIC must send a message response action to NCMS WASHINGTON DC and CMIO NORFOLK VA advising approval or disapproval of request.

(3) Termination of automatic distribution and removal of all COMSEC keying material from account holdings. In addition to actions identified in para 2, accounts must send a message to the Controlling Authorities of all COMSEC keying material that is held in your account requesting disposition instructions for the material. The CONAUTH will respond with disposition of their material (e.g., destroy or transfer). Accounts must submit destruction or transfer reports to their Primary Tier 1 Segment (PT1S) via the X.400 message server. If any COMSEC keying material is to remain in the account the account will be

responsible for all accounting transactions (e.g., destruction and inventory) for the remaining material. If the account removes all COMSEC keying material but maintains their COMSEC equipment they will still be responsible for all accounting transactions for the equipment (e.g., inventory).

(a) Requests for disposition instructions will be addressed as follows:

```
TO:       CONAUTH(S)
          NCMS WASHINGTON DC
INFO:     Chain of Command
          CMIO NORFOLK VA
          DIR TIER1 SAN ANTONIO TX or
          CSLA TIER1
```

SUBJ/REQUEST FOR DISPOSITION OF COMSEC KEYING MATERIAL ICO ACCOUNT NAME (ACCOUNT NUMBER)//
REF/A/DOC/NCMS WASHINGTON DC//
REF/B/GENADMIN/USS UNDERWAY/012311ZDEC09//
REF/C/GENADMIN/COMDESRON TWO EIGHT/031108ZDEC09//
NARR/REF A IS EKMS-1(SERIES). REF B IS TERMINATION REQUEST. REF C IS APPROVAL OF REF B.//
POC/I.B.UNDERWAY/USS GRAYHULL/EKMS MGR/PRI:555-555-1111/EMAIL:UNDERWAYI@DDG-91.NAVY.MIL//
RMKS/1. IRT REF A, REQUEST DISPOSITION OF THE FOLLOWING COMSEC SHORT TITLES:

A. CONAUTH:
B. REASON FOR REQUEST:
C. SHORT TITLES:

(4) Termination of automatic distribution and removal of all COMSEC keying material and COMSEC accountable equipment. In addition to procedures identified in paragraphs 2 and 3; accounts must send a message to NCMS WASHINGTON DC requesting authorization to perform a temporary account-to-account transfer of all COMSEC accountable equipment to a secure storage facility, normally a CRF. NCMS and CMIO space limitations do not permit temporary storage. Transfers to a contractor account must be specifically requested from NCMS and approval received prior to transferring any material to the contractor account. OPNAVINST 2221.5(series) and EKMS 5(series) provide further specific instructions. Transfer transactions must be submitted to your PT1S via the X.400 message server. Prior to transferring the accounts Key Processor (KP) the account must verify with NCMS that all accountable key and equipment have been removed

from the CT-1 data base and there are no items pending. With account in an inactive status and all key and equipment destroyed or transferred the account is no longer required to perform accounting transactions (e.g. destruction or inventory). During this period of inactivity, the COMSEC Account will remain open so it can be readily re-started when the yard period has ended.

(5) Terminating Accounts. Accounts terminating distribution due to disestablishment of EKMS account must follow procedures in chapter 8.

(6) To resume automatic distribution. Notify the CONAUTH, NCMS and CMIO a minimum of 60 days prior to date material will be required. If applicable, submit a request for a Key Processor (KP) to NCMS/CMIO and send a message to NCMS requesting to order for new FIREFLY, MSK, and KG rules. Installation and re-activation of the LMD and KP must be coordinated by the command through the EKMS Technical Support Center. Accounts must ensure the LMD/KP is restored, the account has up to date credentials posted, and the account can connect to the X.400 to receive electronic key.

(a) Requests to resume automatic distribution will be addressed as follows:

TO: NCMS WASHINGTON DC
      CMIO NORFOLK VA
      CONAUTH(s)
INFO: Chain of Command
      DIR TIER1 SAN ANTONIO TX or
      CSLA TIER1

SUBJ/REQUEST TO RESUME AUTOMATIC DISTRIBUTION OF COMSEC KEYING MATERIAL FOR ACCOUNT NAME (ACCOUNT NUMBER)//
REF/A/DOC/NCMS WASH DC//
AMPN/REF A IS EKMS-1(SERIES) ARTICLE 645//

RMKS/1. IRT REF A, REQUEST TO RESUME AUTOMATIC DISTRIBUTION OF COMSEC KEYING MATERIAL:

A. COMMAND NAME:
B. ACCOUNT NUMBER:
C. HCI:
D. DATE MATERIAL REQUIRED:
E. SERVICING DCS STATION:

F. REMARKS:

G. EKMS CREDENTIALS: Date credentials were posted to the X.400 Message Server.

NOTE: Modern FIREFLY Key from the EKMS CF(e.g. STE keys, SDNS keys) is not automatically resupplied and must be ordered by the EKMS Manager, Alternate or other authorized User Representative.

650. ROUTINE MODIFICATION OF AN ACCOUNT ALLOWANCE FOR COMSEC KEYING MATERIAL

a. This article is to be used to acquire COMSEC keying material not previously authorized for receipt by the account (i.e., is not reflected in in COMFLT, TYCOM, or CG area instructions or to support theatre requirements). The Controlling Authority (CONAUTH) must approve the request prior to the commands profile being updated and delivery of the material affected.

b. A routine modification to a commands authorized COMSEC keying material allowance can be met by regular DCS delivery (minimum of 60 days lead-time).

c. Requests will be addressed as illustrated in the following subparagraph.

d. Multiple short titles may be combined and submitted in a single message. Each short title must be assigned separate paragraph and the action addresses for each short title must be clearly identified (e.g. 1. FOR COMSUBPAC, 2. FOR COMMARFORPAC, 3. FOR COMPACFLT) in the case of multiple action addressees.

NOTE: Failure to adhere to the following format could adversely delay keying material acquisition.

(1) USN SURFACE ACCOUNTS SUBORDINATE TO A COMFLT

TO: COMPACFLT PEARL HARBOR HI//N633// or
COMUSFLTFORCOM NORFOLK VA//N023EKMS//
INFO: CONAUTH
ISIC
Chain of Command
NCMS WASHINGTON DC//N3//
CMIO NORFOLK VA//N3//
DIR TIER1 SAN ANTONIO TX or
CSLA TIER1

SUBJ: ROUTINE CHANGE IN COMSEC KEYMAT ALLOWANCE

(2) USN SUBSURFACE ACCOUNTS

TO: COMSUBPAC **or** COMSUBLANT
INFO: CONAUTH
ISIC
Chain of Command
NCMS WASHINGTON DC//N3//
CMIO NORFOLK VA//N3//
DIR TIER1 SAN ANTONIO TX or
CSLA TIER1

SUBJ: ROUTINE CHANGE IN COMSEC KEYMAT ALLOWANCE

(3) USN SHORE ACCOUNTS (LANTFLT UNITS)

TO: CONAUTH
INFO: ISIC
Chain of Command
NCMS WASHINGTON DC//N3//
CMIO NORFOLK VA//N3//
DIR TIER1 SAN ANTONIO TX or
CSLA TIER1

(4) USN SHORE ACCOUNTS (PACFLT UNITS)

TO: COMPACFLT PEARL HARBOR HI//N633//
INFO: CONAUTH
ISIC
Chain of Command
NCMS WASHINGTON DC//N3//
CMIO NORFOLK VA//N3//
DIR TIER1 SAN ANTONIO TX or
CSLA TIER1

SUBJ: ROUTINE CHANGE IN COMSEC KEYMAT ALLOWANCE

NOTE: For keying material in which the JCMO MACDILL AFB FL is the Controlling Authority (CA), the request must include COMPACFLT PEARL HARBOR HI//N633// or COMUSFLTFORCOM NORFOLK VA//EKMS//, as applicable for validation. The JCMO office Will not approve requests which have not been validated by either COMUSFLTFORCOM or COMPACFLT.

(5) COAST GUARD COMMANDS

TO: COGARD C4ITSC ALEXANDRIA VA//BOD-IAB//
INFO: Area and/or District Commander
Chain of Command
NCMS WASHINGTON DC//N3//
CONAUTH
CMIO NORFOLK VA//N3//
DIR TIER1 SAN ANTONIO TX or
CSLA TIER1

SUBJ: ROUTINE CHANGE IN COMSEC KEYMAT ALLOWANCE

(6) MARINE CORPS COMMANDS

TO: Next Senior Flag Level Command (See NOTE below)
INFO: CMC C FOUR CY WASHINGTON DC//
Chain of Command
CONAUTH
NCMS WASHINGTON DC//N3//
CMIO NORFOLK VA//N3//
DIR TIER1 SAN ANTONIO TX or
CSLA TIER1

NOTE: Each USMC Flag Level Command (i.e., DIV, MAW, MLG, MEF) must review and forward their endorsement up the Chain of Command to COMMARFORCOM, PAC or RES//G6//, as appropriate. Ensure that message passing instructions to the G-6 are included (e.g., COMMARFORCOM//G-6//).

SUBJ/ROUTINE CHANGE IN COMSEC KEYMAT ALLOWANCE//
(1) ACCOUNT NUMBER/HCI (E.G. 141126/TS)
(2) SHORT TITLE (E.G. AKAD A5511 880091)
(3) PERMANENT, TEMPORARY, (IF TEMPORARY SPECIFY DURATION 20091001- 20100401)
(4) INCREASE/DECREASE, QUANTITY, JUSTIFICATION (ACCOUNT ESTABLISHMENT/UNIT DECOMMISSIONING / EXERCISE)
(5) PRESENTLY APPROVED ALLOWANCE (IF SHORT TITLE IS NOT HELD, STATE NONE)
(6) REQUIRED ANCILLARY DEVICES (NA FOR KEYING MATERIAL)
(7) DATE MATERIAL REQUIRED (DMR) (I.E. 20091001)
(8) TYCOM/ISIC (REQUIRED ONLY FOR EQUIP AND RELATED DEVICES).
(9) VALIDATION/AUTHORIZATION (CITE CNO AUTHORITY OR EQUIPMENT MASTER PLAN FOR EQUIPMENT AND RELATED DEVICES; NO AUTHORIZATION REQUIRED FOR ONE-FOR-ONE

REPLACEMENT OF DEFECTIVE ITEMS)
(10) SERVICING DCS STATION, ANY SPECIAL SHIPPING INSTRUCTIONS, OR INDICATE OTC PICKUP FROM A VDLS COMPONENT.
(11) POC INFO, NAME, PHONE, EMAILS NIPRNET/SIPRNET
BT

d. Action addees must send a message action to the Controlling Authorities of the material, validating the requirement for the COMSEC short titles requested.

e. The CONAUTH of the COMSEC short title(s) will send a message to CMIO NORFOLK VA and DIRNSA FT GEORGE G MEADE MD, Info NCMS WASHINGTON DC approving or disapproving the request. When approved, CMIO will update the commands allowance profile.

f. NCMS must be notified when an emergency delivery of electronic COMSEC keying material is required. Contact the NCMS Key Division at 240-857-9085 during normal working hours or the NCMS Command Duty Officer at 202-345-3495 after hours or weekends. EKMS accounts must not contact DIRNSA or TIER1 for emergency distribution of COMSEC keying material without first contacting NCMS. NCMS will coordinate with CONAUTH, DIRNSA, TIER1, and CMIO NORFOLK to determine the best method of distribution for emergent keying material requirements. Emergency distribution will only be considered for operational emergencies. EKMS accounts will be required to follow up and send normal required modification of allowance messages.

655. ROUTINE MODIFICATION OF AN ALLOWANCE FOR COMSEC EQUIPMENT, RELATED DEVICES, EQUIPMENT MANUALS AND OPERATING INSTRUCTIONS

1. A request to modify(add/delete a short title or a change in quantity) a command’s ~~the~~ authorized allowance for equipment, related devices, maintenance manuals and operating instructions must be addressed as outlined in this article.

a. Equipment increases - The CNO is the approving authority for any increase in allowance related to COMSEC equipment. Activities must submit a request to the CNO via email or message for action. COMUSFLTFORCOM and COMPACFLT will approve allowance increases for shipboard requirements and will submit such requests to the CNO for final approval and action. If approved, the CNO will notify NCMS or any required action to be taken. If an increase has been validated and assigned a number, the EKMS manager must submit a request to modify the unit’s equipment allowance to NCMS via naval message. NCMS requires a minimum of 30 days before the required delivery date. NCMS will ensure requirements requested match those which have been validated. NCMS cannot provide spares or additional requirements other than those approved and validated by CNO.

NOTE: Neither NCMS nor CMIO Norfolk are funded for the "Overnight" delivery of COMSEC equipment. When expedited delivery is required, any related funding requirements must be provided by the receiving command. This includes material requiring immediate delivery and shipped via; Defense Courier Service (DCS), registered mail, or commercial carrier (FEDEX).

The following is sample message requesting an increase in an activities COMSEC equipment allowance. Correct addresses for such messages are reflected in paragraph 1.b.1 below:

```
MSGID/GENADMIN/UNIT NAME/-/-//
SUBJ/REQUEST FOR INCREASE IN COMSEC EQUIPMENT ALLOWANCE//
REF/A/DOC/NCMS WASH DC/15MAR2010//
AMPN/REF A IS EKMS-1(SERIES) ARTICLE 655//
POC/XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX//
RMKS/1. IAW REF A, THE FOL IS SUBMITTED:
2.  REQUEST NCMS ISSUE THE FOLLOWING EQUIPMENT FOR (GIVE
INSTALLATION INFORMATION) UNDER CNO VALIDATION CMSXX-XXX.
REQUIRED DELIVERY DATE IS XXXX/XX/XX (YEAR/MO/DA).

     SHORT TITLE         QTY

3.  INCLUDE SHIPPING INSTRUCTIONS (AS APPLICABLE), I.E.
FEDEX (ONLY WITHIN THE U.S AND HAWAII), DCS OR OVER THE
COUNTER PICK-UP (FROM CMIO ONLY).  IF NO INSTRUCTIONS ARE
GIVEN, NCMS WILL ASSUME NORMAL REGISTERED MAIL IS
ACCEPTABLE.
```

NOTE: FEDEX shipments require a fixed address (i.e. not FPO/APO address), along with both a POC and telephone number. OTC pickup must be coordinated with CMIO.

b. Equipment decreases - When a COMSEC account has excess COMSEC equipment and/or requires disposition instructions, such will be brought to the attention of NCMS via official naval message. All such requests must also include both the requesting activities ISIC and TYCOM and be submitted in the following format:

```
MSGID/GENADMIN/UNIT NAME/-/-//
```

```
SUBJ/ROUTINE CHANGE IN COMSEC EQUIPMENT ALLOWANCE//
REF/A/DOC/NCMS WASH DC/15MAR2010//
AMPN/REF A IS EKMS-1(SERIES) ARTICLE 655//
POC/XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX//
RMKS/1.  IAW REF A, THE FOLLOWING IS SUBMITTED:
     (A)  ACCOUNT NUMBER/HCI (E.G. 141126/TS)
     (B)  SHORT TITLE (E.G. KG 175, KWR 46)
     (C)  PERMANENT OR TEMPORARY, (IF TEMPORARY, SPECIFY
          THE DURATION E.G. 20091001 - 20100401)
     (D)  INCREASE/DECREASE, QUANTITY, JUSTIFICATION
          (ACCOUNT ESTABLISHMENT, UNIT DECOMMISSIONING,
          EXERCISE) NOTE: FOR DECREASES AND/OR
          DISPOSITION INSTRUCTIONS, THE REQUEST MUST INCLUDE
          THE SERIAL NUMBER FOR ALC 1 ITEMS AND THE QUANTITY
          FOR ALC 2 OR 4 ITEMS.
     (E)  PRESENT APPROVED ALLOWANCE (IF NOT CURRENTLY
          VALIDATED FOR/HELD BY ACCOUNT, HELD, STATE NONE)
     (F)  REQUIRED ANCILLARY DEVICES (NA FOR DECREASES)
     (G)  DATE MATERIAL REQUIRED (I.E. 20100501 OR NA FOR
          DECREASES)
     (H)  TYCOM/ISIC (REQUIRED ONLY FOR EQUIP AND RELATED
          DEVICES).
     (I)  VALIDATION/AUTHORIZATION (CITE CNO AUTHORITY OR
          EQUIPMENT MASTER PLAN FOR EQUIPMENT AND RELATED
          DEVICES; NO AUTHORIZATION REQUIRED FOR ONE-FOR-
          ONE REPLACEMENT OF DEFECTIVE ITEMS)
     (J)  SERVICING DCS STATION, ANY SPECIAL SHIPPING
          INSTRUCTIONS, OR INDICATE OTC PICKUP FROM A VDLS
          COMPONENT.
     (K)  POC INFO, NAME, PHONE, NIPRNET/SIPRNET ADDRESS
     2.  REQUEST DISPOSITION INSTRUCTIONS FOR THE ITEMS
     REFLECTED IN PARA 1.B ABOVE (ONLY APPLICABLE FOR
     DECREASES AND/OR DISPOSITION REQUESTS.  OTHERWISE PUT
     NA IN PARAGRAPH 2.
     3.  ADDITIONAL COMMENTS: XXXXXXXXXXXXXXXXXXXXXXXXX//
     BT
```

NOTE: COMSEC equipment will NOT be destroyed without NCMS authorization. An example message has been provided. Messages received without the minimum information reflected below will delay in responding to the request.

(1) <u>EQUIPMENT AND RELATED DEVICES</u>:

(a) <u>Navy and MSC Commands</u>:

ACTION: NCMS WASHINGTON DC//N3//
CNO WASHINGTON DC
INFO: ISIC
Chain of Command
CMIO NORFOLK VA//N3//
DIR TIER1 SAN ANTONIO TX <u>or</u>
CSLA TIER1
SPAWARSYSCEN ATLANTIC CHARLESTON SC

(b) <u>Coast Guard Commands</u>:

ACTION: COGARD C4ITSC ALEXANDRIA
VA//BOD-IAB//
INFO: Area and/or District Commander
NCMS WASHINGTON DC//N3//
CMIO NORFOLK VA//N3//
DIR TIER1 SAN ANTONIO TX <u>or</u>
CSLA TIER1
SPAWARSYSCEN ATLANTIC CHARLESTON SC

(c) <u>Marine Corps Commands</u>: Per Article 605.b. NOTE 1 (Green Dollar)

ACTION: Next Senior Flag Level Command (See NOTE below)
INFO: CMC C FOUR CY WASHINGTON DC//
Chain of Command
COMMARCORSYSCOM QUANTICO VA//CINS//
CG MARCORLOGCOM ALBANY GA
NCMS WASHINGTON DC//N3//
CMIO NORFOLK VA//N3//
DIR TIER1 SAN ANTONIO TX <u>or</u>
CSLA TIER1
SPAWARSYSCEN ATLANTIC CHARLESTON SC

(d) CG MARCORLOGCOM ALBANY GA for requesting deficiencies and disposition of excess COMSEC equipment, CG MCCDC QUANTICO VA for change to T/E allowances.

NOTES: 1. In addition to the above, USMC accounts must consult and follow service specific guidance in requesting a Modification of Allowance (MOA) for COMSEC Table of Equipment (T/E) allowances.

2. Each USMC Flag Level Command (i.e., Div, MAW, MAW, MLG, MEF) must review and forward their endorsement up the Chain of Command to COMMARFORCOM, PAC <u>or</u> RES//G-

6//, as appropriate. Ensure that message includes COMMARFORCOM //G-6//.

3. COMMARFORCOM, PAC and RES endorsements on requests from FMF Commands and requests from supporting establishment commands must be submitted to: CMC C FOUR CY WASHINGTON DC//, CHAIN OF COMMAND, NCMS WASHINGTON DC//N3//.

4. The procedures for modifying allowances of COMSEC equipment and related devices, on a routine and emergency basis that are detailed in this Article and in Article 675 are not applicable to USMC Commands subordinate to COMMARFORCOM/PAC/RES, and USCGs at the Marine Expeditionary Force (MEF), Marine Division (DIV), Marine Aircraft Wing (MAW), and Marine Logistics Group (MLG) levels. Marine aviation organizations whose COMSEC equipment is not authorized by and established in a T/E and is in direct support of “Blue Dollar” Navy (Non-T/E Systems and Aircraft) must follow procedures delineated for “Navy Commands” in Article 605a.

5. For USCG accounts: The disposition of CCI equipment, with exception to the LMD/KP USCG accounts will submit requests action to COGARD C4ITSC ALEXANDRIA VA//BOD-IAB// and info NCMS on such requests. Disposition requests involving a LMD/KP will be sent action to NCMS and info COGARD C4ITSC ALEXANDRIA VA//BOD-IAB//.

(2) EQUIPMENT MANUALS and OPERATING INSTRUCTIONS:

ACTION: NCMS WASHINGTON DC//N3//
INFO: ISIC
CMC C FOUR CY WASHINGTON DC//
(USMC commands only)
COMMARCORSYSCOM QUANTICO VA//CINS//
(USMC commands only)
COGARD C4ITSC ALEXANDRIA VA//—//BOD-IAB//
(USCG commands only)
Area and/or District Commander
(USCG commands only)
Chain of Command
CMIO NORFOLK VA//N3//
DIR TIER1 SAN ANTONIO TX or
CSLA TIER1

b. Action addressees must approve, disapprove, or modify a request for routine modification from the account by sending a message to NCMS//N3//, except for COMMARFORCOM, PAC and RES, info to the remaining addressees on the original request.

c. NCMS//N3// must be an addressee on all correspondence involving the permanent transfer of COMSEC equipment, related devices, maintenance manuals, and operating instructions.

660. FORMAT FOR ROUTINE MODIFICATION OF AN ACCOUNT ALLOWANCE

a. As outlined in Articles 650 - 655 above.

665. FORMAT FOR REQUESTING STANDARD DEPLOYMENT ALLOWANCE AND/OR ISSUANCE OF DUAL MEDIA

a. Requests for dual media (physical **key tape** and **electronic key**) standard deployment keymat, as listed in the COMFLT, TYCOM, or CG area instructions, must be submitted a minimum of 60 days before departure from homeport. CMIO will respond to requests for electronic key within 48 hours.

b. The following format must be used to request standard deployment keymat and to also indicate partial reductions in the quantity of standard deployment keymat. Where information for a particular item is not applicable, insert "N/A."

```
TO:   CMIO NORFOLK VA (See NOTE below)
INFO: CONAUTHs
      COMFLTs
      ISIC
      NCMS WASHINGTON DC//N3//
      DIRNSA FT GEORGE G MEADE MD
      DIR TIER1 SAN ANTONIO TX or
      CSLA TIER1
      MSGID/GENADMIN/CMIO NORFOLK/-/-//
      SUBJ/DEPLOYMENT ALLOWANCE//
      REF/A/DOC/NCMS WASH DC/-//
      AMPN/REF A IS EKMS-1(SERIES)//
      RMKS/1. IAW REF A, THE FOL IS SUBMITTED:

        (1)  ACCOUNT NUMBER/HCI (e.g. 130061/TS).

        (2)  SHIP TYPE (E.G., FFG, CG, CVN, SSN).

        (3)  DEPLOYMENT AREA (E.G., IO, AG, SOH, WP,
             MED, LANT).
```

(4) DATE MATERIAL NEEDED (E.G., 20091030).

(5) INCLUSIVE DATES MATERIAL REQUIRED: 20091101 20100430).

(6) CITE APPLICABLE INSTRUCTION/AUTHORIZATION.

(7) ANY SPECIAL MATERIAL REQUIRED OR ANY SPECIAL REQUIREMENTS (E.G., PARTIAL REDUCTION(S)).

(8) SERVICING DCS STATION, ANY SPECIAL SHIPPING INSTRUCTIONS, OR INDICATE OTC PICKUP FROM A PMHS OR A VDLS COMPONENT.

(9) POC INFO, PHONE, EMAIL ADDRESS (NIPRNET/SIPRNET).

NOTE: COMSUBFOR or COMSUBPAC will submit requirements to CMIO Norfolk for deploying submarine accounts.

670. REQUESTING A FIREFLY VECTOR SET OR MESSAGE SIGNATURE KEY (MSK)

a. Prior to requesting either a new FIREFLY, MSK, or both the EKMS Technical Support Center (1-877-NAV-EKMS) must be contacted to determine if the system can be restored without the need to acquire a new FF Vector Set or MSK key. The format to be used in requesting either a new FF Vector Set, MSK, or both is reflected below:

```
FM ORIGINATING COMMAND
TO NCMS WASHINGTON DC
INFO ISIC
MSGID/GENADMIN/USS GRAYHULL/-/-//
SUBJ/REQ FOR NEW FIREFLY AND/OR MSK
REF/A/DOC/NCMS WASH DC/-/-//
AMPN/REF A IS EKMS-1(SERIES)//
RMKS/1. IAW ARTICLE 670 TO REF A, THE FOL IS PROVIDED:
(1) TYPE OF KEY REQUIRED (FF VECTOR SET, MSK, OR BOTH)
     NOTE: FOR NEW ACCOUNTS, INCLUDE (2) KSV-21 CARDS WITH
     EKMS PRIVILEGES IN PARA 1.
(2) QUANTITY (NORMALLY TWO COPIES)
(3) COMMAND NAME
(4) EKMS ACCOUNT NUMBER
(5) EKMS MANAGER NAME, TELEPHONE NUMBER, AND NIPRNET EMAIL
```

ADDRESS.

(6) REASON FOR REQUEST (I.E. KP FAILURE, FAILURE TO CONDUCT KP REKEY) AND DATE EKMS TECHNICAL SUPPORT CENTER CONTACTED.

(7) SEED OR OPERATIONAL (JUSTIFICATION MUST BE PROVIDED FOR OPERATIONAL KEY)

(8) METHOD OF SHIPMENT (THERE ARE THREE METHODS OF SHIPMENT DEPENDING ON CIRCUMSTANCES. NORMAL MOVEMENT OF EKMS KEY IS VIA DCS WITH ALL SHIPMENTS ORIGINATING FROM THE CENTRAL FACILITY EACH FRIDAY. UNLESS OTHERWISE DIRECTED, KEY WILL BE SHIPPED VIA DCS. KEYS MAY ALSO BE SHIPPED VIA FEDEX PROVIDED YOU HAVE A VALID FEDEX CONUS SHIPPING ADDRESS AND PROVIDE A POC AT THE SHIPPING ADDRESS. THE CENTRAL FACILITY WILL CALL TO VERIFY THE POC IS AWARE THAT KEY IS BEING DELIVERED. THE CENTRAL FACILITY DOES NOT SCHEDULE FEDEX ON FRIDAYS. ELECTRONIC SHIPPING IS AVAILABLE IF ANOTHER EKMS ACCOUNT EXISTS IN PROXIMITY AND THE EKMS MANAGER IS WILLING TO DOWNLOAD THE KEY ELECTRONICALLY. TO DO SO, THE EKMS MANAGER WILL HAVE TO REGISTER THE ACCOUNT AS A LOCAL ELEMENT, DOWNLOAD THE KEY TO A KSD-64A, AND ISSUE THE KEY ON A LOCAL CUSTODY BASIS TO YOUR COMMAND. THIS IS RESERVED FOR EMERGENCIES ONLY SUCH AS WHEN AN ACCOUNT IS DEPLOYING WITHIN 48 HOURS. YOU MUST PROVIDE THE NAME AND EKMS ID OF THE ACCOUNT WILLING TO ACCEPT THE KEY AND POC INFORMATION FOR THE MANAGER. ADDITIONALLY, IN THIS SCENARIO THE EKMS MANAGER OF THE ACCOUNT RECEIVING THE KEYS VIA KSD-64A MUST; PREPARE A LOCAL DESTRUCTION RECORD REFLECTING THE FF VECTOR SET AND MSK WHEN LOADED AND AFTER CREATION OF THE REINIT1 AND NAVREINIT2 CIKS, MUST ZEROIZE THE KSD-64As THE FF VECTOR SET AND MSK WERE PROVIDED ON, SIGN AND DATE (WITH A WITNESS) THE DESTRUCTION REPORT AND RETURN IT TO THE EKMS MANAGER OF THE ACCOUNT THAT ISSUED THE FF VECTOR SET AND MSK.

NOTE: Failure to provide a destruction report to the account which issued the FF Vector Set and MSK will result in these items remaining on-charge to the issuing account and prevent the proper recording of the use of these keys as destroyed as required by National and Navy policy as stated in the Operational Security Doctrine for the LMD/KP and Article 238 of this manual.

672. FORMAT AND ADDRESSEES FOR REQUESTING NEW KEYING MATERIAL

a. The majority of new operational requirements may be satisfied by allocating keymat that is readily available, but not yet designated for a specific purpose. In this situation, the keymat can be provided in a relatively short time (e.g., 2-30 days dependent on location and/or delivery options). The opposite case would be a situation, which would require that the National Security Agency produce a completely new paper-based short title of keymat, requiring a minimum of 120 days notice. In view of ongoing efforts to eliminate Punched Paper Tape keying material, NCMS will not approve any request for Punched Paper Tape keying material intended for U.S. only use. U.S. only key will be produced and distributed in electronic form only.

NOTE: LMD/KP-equipped EKMS accounts are authorized to generate AL Code 7 key locally without prior authorization from NCMS. EKMS 704 (series) contains a list of equipment types the KP is capable of producing key for. EKMS accounts are encouraged to generate their own AL Code 7 key for cryptonets of 10 or less nodes. Accounts generating key locally must adhere to the guidance set forth for Controlling Authorities outlined in Annex C.

b. The following format must be used to request assignment of a new short title of electronic/paper-based keymat to support a new or revised operational requirement. Where information for a particular item is not applicable, insert "N/A." Address the request as follows:

(1) Navy (see NOTE below), MSC, and USMC

TO: NCMS WASHINGTON DC//N3//

INFO: CMC C FOUR CY WASHINGTON DC//
(USMC commands only)
Chain of Command

DIR TIER1 SAN ANTONIO TX
CSLA TIER1
CMIO NORFOLK VA//N3//
DIRNSA FT GEORGE G MEADE MD//I31//(Add DP22 for foreign releasable key)

NOTE: USN surface accounts subordinate to a COMFLT will address their request action to COMPACFLT PEARL HARBOR HI//N633// or COMUSFLTFORCOM NORFOLK VA//N023EKMS// info ISIC, Chain of Command, NCMS WASHINGTON DC//N3//, CMIO NORFOLK VA//N3// and DIRNSA FT GEORGE G MEADE MD.

(2) Coast Guard Commands:

```
    ACTION:  COGARD C4ITSC ALEXANDRIA VA//BOD-IAB//
    INFO:    Area and/or District Commander
             Chain of Command
             NCMS WASHINGTON DC//N3//
             CMIO NORFOLK VA//N3//
             DIR TIER1 SAN ANTONIO TX
             CSLA TIER1
             DIRNSA FT GEORGE G MEADE MD//I31//(Add
             DP22 for foreign releasable key)
```

(3) Marine Corps FMF Commands:

```
    ACTION:  COMMARFORCOM, PAC OR RES
    INFO:    CMC C FOUR CY WASHINGTON DC//
             Chain of Command
             NCMS WASHINGTON DC//N3//
             CMIO NORFOLK VA//N3//
             DIR TIER 1 SAN ANTONIO TX
             CSLA TIER1
             DIRNSA FT GEORGE G MEADE MD//I31//(Add
             DP22 for foreign releasable key)
```

```
MSGID/GENADMIN/UNIT NAME/-/MONTH//
SUBJ/REQUEST FOR TRADITIONAL NEW KEYMAT SHORT TITLE//
REF/A/DOC/NCMS/05APR2010//
AMPN/REF A IS EKMS-1(SERIES)//
POC/XXXXXXXXXXXXX/ (RANK)/TEL/ (XXX) XXX-XXXX/DSN:XXX-
XXX-XXXX/EMAIL: XXXXXXXXXXXXXXXXXX//
BT
CLASSIFICATION: (AS APPLICABLE)
SUBJ/REQUEST FOR NEW TRADITIONAL KEYING MATERIAL//
POC/XXXXXXXXXXXXX/ (RANK)/TEL/ (XXX) XXX-XXXX/DSN: XXX-
XXXX/EMAIL: XXXXXXXXXXXXXXXXXX//
RMKS/1.  IAW REF A, REQUEST ASSIGN COMSEC KEYING
MATERIAL IN SUPPORT OF NEW REQUIREMENT (EXERCISE, NEW
EQUIPMENT OR ETC).
2.  THE FOLLOWING INFORMATION IS PROVIDED:
PART I
  A.  IF THIS IS A CONVERSION OF AN EXISTING PHYSICAL
  SHORT TITLE PLEASE PUT THAT SHORT TITLE HERE AND SKIP
  TO K (IMPLEMENTATION DATE)
  B.  EQUIPMENT TYPE: (I.E. KIV-7, KY-58, KYV-5 ETC.)
  C.  ALLIED OR US: (IF ALLIED RELEASABLE TO WHOM?  I.E.
  AUS, CAN, NLZ, UK ETC)
  D.  KEY PURPOSE: (I.E. OPERATIONAL, TEST, MAINTENANCE,
  EXERCISE ETC.)
```

```
          E.  KEY USE:  (KEK, TEK, AEK ETC.)
          F.  ALC: 1 (PHYSICAL (OPTION/RELEASABLE) OR 6
          (ELECTRONIC)
          G.  CLASSIFICATION: XXXXXX
          H.  SUPERSESSION RATE: XXXXXXXX
          I.  CRYPTOPERIOD: XXXXXXX (PLEASE PUT THE CORRECT
          DIGRAPH IF KNOWN, I.E. AA (31 SEGMENTS/DAILY
          CRYPTOPERIOD; ZB 15 SEGMENTS, 5 COPIES EACH, 75 TOTAL,
          WEEKLY CRYPTOPERIOD)
          J.  DESIRED IN PLACE DATE: XXXXXXXXXXXXXXXXXXXX
          K.  IMPLEMENTATION DATE: XXXXXXX (OPTIONAL : IF THIS
          IS CONVERSION OF AN EXISTING PHYSICAL SHORT TITLE
          PLEASE INDICATE WHICH EDITION YOU WANT THE ELECTRONIC
          VERSION TO START WITH)
          L.  DISTRIBUTION:
              ACCOUNTS QTY
               1. XXXXXX XX
               2. XXXXXX XX
          M. (THIS WILL BE THE COMMAND THAT WILL HAVE
          OPERATIONAL MANAGEMENT RESPONSIBILITY FOR THE NEW
          KEYMAT.  IF THE REQUESTING COMMAND IS NOT THE
          CONAUTH, PROVIDE MESSAGE PLA AND THE OFFICE CODE OF
          THE CONAUTH).

PART II
     (RELEASABLE COMPATIBILITY)
BT
```

c. Action addressee must approve, disapprove, or modify a request by a command for a new keymat short title by sending a message to NCMS WASHINGTON DC//N3//, info to the remaining addressees on the original request.

675. **EMERGENCY MODIFICATION OF AN AUTHORIZED ALLOWANCE**:

a. An emergency modification of the authorized allowance of a command is one that requires the immediate transfer of COMSEC material to satisfy an urgent and unforeseen operational requirement (as determined by the Commanding Officer).

NOTE: USMC commands must refer to Article 605 for temporary transfers of equipment, and Article 655.a.(1)(c) for modification of allowance of equipment and related devices.

b. Commanding Officers are authorized to direct the temporary transfer of COMSEC material between EKMS accounts to satisfy urgent and unforeseen operational requirements.

c. Temporary transfers of COMSEC equipment will be in accordance with Article 401.b to EKMS-5(series). Regardless of format, temporary transfer of keying material is restricted to no more than two editions and a period not to exceed three months. The temporary transfer is authorized within the following constraints:

(1) The transferring command must not reduce their holdings below the minimum necessary to meet known or reasonably anticipated operational requirements.

(2) The recipient of the material is authorized to hold the material as part of their normal authorized allowance.

d. CRFs and afloat commands holding provisional spare equipment are authorized to transfer COMSEC equipment and related devices as a replacement for failed equipment submitted in a casualty report (CASREP).

e. After initiating an emergency temporary transfer of material, the transferring command must submit a message to the following addressees providing EKMS account numbers; short title(s) of COMSEC material transferred; and the rationale for the emergency transfer:

TO: CONAUTH (See NOTE below)
INFO: COMPACFLT PEARL HARBOR HI//N633// or
COMUSFLTFORCOM NORFOLK VA//N023EKMS//
CMC C FOUR CY WASHINGTON DC//
(USMC commands only-for keying material)
COGARD C4ITSC ALEXANDRIA VA//BOD-IAB//
(USCG commands only)
Area and/or District Commander
(USCG commands only)
ISICs (transferring and receiving accounts)
Recipient of material
NCMS WASHINGTON DC//N3//
CMIO NORFOLK VA //N3//

Subject: EMERGENCY TRANSFER OF COMSEC MATERIAL

f. Transferring commands must cite this Article and request by the originating command (e.g., message, phone call) in the body of the SF-153 as authorization for an emergency transfer of AL Code 1, 2, or 6 material. (Document the transfer of AL Code 4 and 7 material locally).

680. PERMANENT TRANSFER OF AFLOAT COMMANDS TO A NEW OPERATING AREA (OPAREA):

a. Afloat commands which are permanently re-locating to a homeport in a different ocean area must inform NCMS and CMIO of new OPAREA material requirements 60 days prior to departure from their present homeport.

b. The request will be addressed as follows:

TO: CMIO NORFOLK VA//N3//
INFO: COMPACFLT PEARL HARBOR HI//N633// or
COMUSFLTFORCOM NORFOLK VA//N023EKMS//
TYCOMs and/or ISICs (both areas)
COGARD C4ITSC ALEXANDRIA VA //BOD-IAB// **(USCG commands only)**
CONAUTHs
NCMS WASHINGTON DC//N3//

c. The request must be formatted as detailed in Article 665.b. and include stop date, YYMM, for material provided for present OPAREA and start date, YYMM, for material for the new OPAREA.

d. Upon arrival at the new homeport, the account must:

(1) Coordinate with applicable DCS commands to effect the change of the servicing DCS station (if not previously done).

(2) Obtain disposition instructions from the CONAUTHs for the keying material held/used in the previous OPAREA. If authorized for destruction, cite applicable authorization on the corresponding destruction documents. Ensure destruction reports are submitted to NCMS in accordance with Chapter 7 to ensure the material is removed from charge to the account.

CHAPTER 7 -- CONTROL AND DOCUMENTATION REQUIREMENTS FOR COMSEC MATERIAL

FIGURES:

CHAPTER 7 - CONTROL AND DOCUMENTATION REQUIREMENTS FOR COMSEC MATERIAL

701. GENERAL:

a. The sensitivity of COMSEC material necessitates the need for training, active account involvement, attention to detail and detailed procedures. COMSEC material must be controlled and properly accounted for at all times.

b. This chapter provides procedures for maintaining the integrity and control of accountable COMSEC material from receipt to disposition (i.e., transfer or destruction).

c. **Accuracy** in the preparation of accounting documents is an **extremely important** aspect of account management.

AMD-9

d. If, at **any** time, you, as either an EKMS Manager or LE responsible for COMSEC material, are unsure of how to handle a particular requirement or situation, you are strongly encouraged to contact your EKMS Manager, ~~CMS A&A Training~~ COR Audit Team, or NCMS for assistance.

NOTE: Annex S **contains points of contact information.**

703. REQUIRED COMSEC FILES:

Each EKMS account will establish and maintain the following COMSEC-related files:

a. Chronological File.

b. Correspondence, Message and Directives File.

c. General Message File.

d. Local Custody File.

NOTES: 1. If any of the required files are too large for one file or folder, they may be divided into multiple files.

2. LE files will contain copies of reports, messages, and correspondence that the EKMS Manager has determined to be necessary for the effective management of a LE. Specific LE file requirements are discussed in

this chapter.

706. COMSEC CHRONOLOGICAL FILE:

a. **The Chronological File** must be used to maintain the following:

(1) COMSEC material accounting reports (e.g. receipt, transfer, destruction, generation, conversion, possession, relief from accountability, inventories etc.), excluding reports maintained in the Local Custody File and reports properly disposed of after their required retention periods (e.g., Local Destruction Record, LE issue).

(2) An up-to-date printout of Accountable Items Summary (AIS). **At the account level, either a printed up-to-date Change of Account Location (COAL) inventory or AIS may be maintained as discussed in Article 763.c (note).**

NOTE: Non-COMSEC accountable items, e.g. hard drives, publications, backup tapes, etc… will NOT be accounted for or tracked within LCMS. If non-COMSEC accountable items in LCMS are discovered, such must be reported and documented in accordance with Article 1005.

(3) Inventory reports. Retain in accordance with Annex T.

(4) Transaction Status Logs. Transaction Status Logs are used to record and assign a sequential transaction number (TN). LCMS maintains the TN log and assigns a TN for each computer interaction.

(5) CMS Form 1 and/or USTRANSCOM Form 10.

(6) SD 572 Forms for all account COMSEC users.

(7) Key Conversion Notices (KCN)

(8) EKMS Central Facility (CF) Notices

(9) The following CF forms:

CF Form 1206 (User Representative Registration Request)

CF Form 1205 User Representative Partition Privilege Registration Request

CF Form 1050 Secure Data Network System (SDNS) Key Order requests

NOTE: Although the forms identified in paragraph 9 no longer require "wet" signatures and may be submitted and processed electronically, they will be printed out and filed in the Chronological file to provide verification during training visits and ~~inspections~~ audits that an adequate number of personnel having ordering privileges for the account.

AMD-9

b. **Record copies**: Record copies in the Chronological File must be original or exact duplicates of the originals and must include both dates and signatures.

c. **Working copies**: Working copies of inventory and destruction reports must be retained in accordance with Annex T. The definition of a working copy can be found in Annex A.

709. CORRESPONDENCE, MESSAGE, AND DIRECTIVES FILES:

a. **The Correspondence File** must be used to maintain the following:

(1) EKMS account registration correspondence.

NOTE: Mandatory for accounts established after 01 Jul 1993; optional for previously established accounts.

(2) Appointment correspondence. These include letters for EKMS Managers, Alternates, Clerks and LEs (Issuing) (See Annex J for an example of an Appointment Letter).

(3) COMSEC incident and PDS reports.

(4) Correspondence relating to command allowance and authorization to store classified COMSEC material.

AMD-9

(5) The last ~~ISIC inspection~~ COR Audit Report.

(6) A list of personnel authorized access to keying material and the LMD/KP, designated in writing by the current Commanding Officer or SCMSRO.

AMD-9

(7) Spot checks. Spot checks must be retained for 2 years or until completion of the next ~~ISIC inspection~~ COR Audit.

(8) All documentation of training conducted.

(9) Logs pending destruction (i.e. Audit logs, Visitors logs).

b. **The Message File** must contain a copy of all effective general messages (e.g., ALCOMs, ALCOMLANT ALFAs, ALCOMPAC Ps) that pertain to account holdings or COMSEC policy and procedures (e.g., Controlling Authority status messages).

c. **The Directives File** must contain a copy of each effective command higher authority directive that relates to COMSEC matters (e.g. guidance for LEs, Letters of Agreement (LOA), and waivers of COMSEC policy and procedures).

712. LOCAL CUSTODY FILE:

The Local Custody File must contain all effective signed local custody documents for material which is issued.

AMD-9

a. **Requirement for Local Custody Issue (LCI) documents**: For **every** issue of accountable material there must be a corresponding LCI document. Other accounting documents shall not be substituted for LCI documents ~~except as authorized in the note below~~. Failure to have LCI documents or equivalent for materials issued must be reported as a Physical Incident in accordance with Chapter 9.

AMD-9

~~**NOTE: For effective file management purposes, on a semi-annual basis, EKMS Managers are authorized to generate an inventory for LEs issued material from LCMS and have (2) personnel at the LE level conduct a complete inventory of all material issued and sign/return the inventory to the EKMS Manager. A copy of the inventory will also be maintained at the LE level. After verification of the inventory, EKMS Managers and the LE are authorized to purge the individual SF-153s previously used to maintain local custody of the material reflected. Inventories used for this purpose will not be signed or witnessed by the EKMS Manager or Alternates but by the LE (work center) having custody of the material. This practice does not imply that during the period between inventories described that LCI documents are not required. Both EKMS Managers and LE personnel will maintain LCI documents except as authorized by this article.**~~

b. **Control**: EKMS Managers and LEs must maintain physical control over their local custody documents since this file contains the only documentation of COMSEC material issued locally.

c. **Completeness**: The Local Custody File must contain a signed document (i.e., SF-153 or locally prepared equivalent form) for each item of COMSEC material charged to the account which has been issued to authorized LEs. Material issued to personnel who have signed for COMSEC material who go on leave or TAD in excess of 30 days or who transfer, are reassigned or retire must be returned within LCMS to the EKMS Manager and reissued. See article 455.m and Annex K Para 4 for additional information.

NOTE: For electronic key which cannot be returned to the EKMS Manager for reissue from LCMS, the LCI document will be amended by lining out the original recipient(s) in blocks 15 or 16, as applicable, initialing the line-out and the material signed for by the new recipient(s). Alternatively if space is not available, a SF-153 may be created outside of LCMS which reflects the same data as the original and signed by the new person signing for the material. Any editions previously issued which have superseded and been destroyed will be lined out if the first procedure is used or not reflected on the new SF-153 if the later method is used. In either case, a copy of the edited or new SF-153 will be on file with both the EKMS Manager and the LE.

d. **Signature Requirements**: Local Custody documents reflecting TS material will always require two signatures. Unless directed by local, ISIC, or TYCOM policy only one signature is required for Local Custody documents for Secret and below material, unkeyed CCI equipment or CCI equipment keyed with Secret and below material. Electronic signatures are acceptable, provided all legal requirements (e.g., authenticity, non-repudiation, verification, and records management/storage) are met. Legal requirements include, but are not limited to, Article 15 U.S.C. 7001, 7006 and 7021. DOD CAC or NSS PKI Tokens meet these requirements.

NOTE: This includes TS key loaded into an electronic storage or issuing devices.

715. HANDLING, STORAGE, RETENTION, AND CLASSIFICATION OF COMSEC FILES, RECORDS, AND LOGS:

a. **Handling and storage**: COMSEC files, records, and logs must be handled and stored in accordance with their overall classification and, when possible, may be stored electronically. Documents requiring signatures must be in hard copy form. These items are not COMSEC material.

b. **Retention periods**: Annex T contains the minimum retention periods for COMSEC files, records, and logs.

c. **Inactive records**: When placed in an inactive status, COMSEC files, records, and logs must be clearly labeled with the appropriate classification and the authorized date of destruction. When practical, all material to be destroyed during the same general timeframe should be grouped together, e.g., material authorized for destruction based on a retention period of two years. **For example: Chronological files for the year 2007 may be destroyed 1 January 2010 or later.**

d. **Classification guidance**:

(1) The following will be classified at a minimum of CONFIDENTIAL:

(a) Reports that list two person control (TPC) material. (Guidance can be found in CJCSI 3260.01(series)).

NOTE: Reports containing a complete or nearly complete record of an account's classified keying material holdings are "UNCLASSIFIED/FOR OFFICIAL USE ONLY", provided such reports/records do not list short titles that require a minimum classification of CONFIDENTIAL (e.g., TPC material or those which reflect status information, or other comments derived from classified sources, etc..)

(b) Reports that indicate the effective date of classified keying material.

(2) The following additional general guidance is provided:

(a) Although individual reports (e.g., receipt, transfer, conversion, destruction) are "For Official Use Only" (FOUO), a file holding a classified report must be classified accordingly.

(b) Any report or file containing classified information will be classified according to the highest classification of the information contained therein. **Except as indicated below, all COMSEC incident messages will be classified a minimum of CONFIDENTIAL.**

NOTE: Incident reports will be classified at a minimum of confidential unless related to UNCLASSIFIED Data Encryption System (DES) material. If necessary, EKMS Managers are to consult with NCMS (N5) prior to transmitting Incident reports if in doubt about the appropriate classification to assign.

(c) All files and/or records containing classified COMSEC or COMSEC-related information will be classified appropriately and will reflect:

"Derived from: EKMS 1 (series)
“Declassify on: DD Month YYYY”

Note: The use of X1 – X8 is prohibited for downgrading /declassifying classified information. Declassification /Downgrading instructions will be in accordance with the CNO Policy ltr Ser N09N2/8U223000 dated 7 Jan 2008 until incorporated into SECNAV M5510.36. For records marked on/after 22 Sep 03, the date shown above reflects 25 years from the last authorized use of X1 – X8.

(d) Classification is the responsibility of the EKMS Manager and must be determined by evaluating the content of each report or file. If in doubt, consult SECNAV M5510.36 (series) or contact NCMS (N5) for guidance.

718. USE OF FORMS AND MAGNETIC MEDIA:

a. **Locally prepared**: Locally prepared forms may be created at the discretion of a command when the command does not have a LMD using LCMS. Locally prepared forms must contain the same information, including signature data, as those produced by LCMS. For LCI documents and required content, see Article 769.c

b. **Computer generated:** EKMS accounts equipped with a LMD are required to use LCMS to maintain all COMSEC material held by the account. If additional computer-generated forms are desired by the account, such as using spreadsheets or other software, a separate computer must be used. Only LCMS software may be installed in the LMD. Removing the LMD hard drive containing LCMS and replacing it with a hard drive containing non-LCMS software is prohibited.

(1) Commands that maintain computer generated records should keep an up-to-date back up at all times.

(2) Users of LCMS will retain copies of their Transaction Status Log in accordance with Annex T.

(3) The requirements for signatures, where required, may not be waived. Computer generated records must allow for signatures on printouts.

(4) Computer generated forms that would normally have material lined out must either allow for a separate area for lined out items or have an extra column to indicate that the item has been lined out. Items that would normally be lined out must not be deleted until the retention times in Annex T have been met.

c. **Back-up media**: Any magnetic media (e.g. hard disk, magnetic tape, etc.) can become corrupted by a variety of things such as spikes, static, power surges, magnets, etc. To protect against the potential loss of critical accounting data, commands will ensure backups are conducted as noted below.

NOTES: 1. All commands must use a minimum of two magnetic tapes to back up the LCMS database and for root back-ups.

2. Tapes must be alternated and replaced annually to minimize the loss of data due to tape failure from frequent use. All back-up tapes will reflect; the date of the backup, a description of the backup, i.e. /u/usr or /root and also reflect the appropriate classification and downgrading instructions in accordance with in Article 715.d.2.c above.

3. Backup media used is not COMSEC accountable and will be stored, safeguarded and accounted for in accordance with SECNAV M5510.36 (series) and local directives.

d. **LCMS Back-up Requirements**: Database maintenance for EKMS accounts will be conducted as described below:

(1) LCMS Database: A back up of the LCMS Database will be performed at the end of each computer session that modifies the Accountable Item Summary and/or Transaction Status (TN) Log.

(2) LCMS UNIX Applications (/u/usr): LCMS uses various applications that are stored in the /u/usr directory on the LMD. The /u/usr backup must be performed when the system is first installed and monthly thereafter.

(3) Root: The backup of the SCO UNIX operating system UNIX account information is accomplished by performing a Root backup. The Root backup must be performed when the system is first installed and monthly thereafter.

(4) Emergency Start-up Disks: During initial LMD/KP installation at each account, the account must create an emergency start-up disk, and an emergency file systems disk. In the event of catastrophic system failure, the emergency start-up disk enables the operator to boot the computer from a floppy disk. The emergency file system disk allows the operator to mount the system files that will allow the operator to load the three backup tapes mentioned above.

> **NOTE: Failure to perform backups as described above is a Practice Dangerous to Security (PDS) in accordance with Chapter 10.**

721. COMSEC LIBRARY:

All EKMS accounts must maintain a COMSEC Library which, consists of the following manuals and instructions:

> **NOTE: EKMS Managers must also ensure that their LE commands have access to or are provided copies of all COMSEC manuals and instructions required by the LE. Documents indicated with an asterisk (*) can be found on the NCMS SIPRNET Collaborative At-Sea (CAS) portal.**

a. EKMS-704 * - LMD/KP Operator’s manual.

b. EKMS Manager JQR *.

c. COMLANTFLT/COMPACFLT/COMUSNAVEURINST C2282.1 (series) – Basic Shipboard Allowance of COMSEC Material.(Surface ships only) Can be obtained from COMUSFLTFORCOM at(757) 836-5853 or via SIPRNET at: www.ffc.navy.smil.mil.

d. EKMS 1 (series)* - EKMS Policy and Procedures Manual for EKMS Tiers 2 and 3.

e. EKMS 3 (series)* - EKMS Inspection Manual.

f. EKMS 5 (series)* - Cryptographic Equipment Manual.

g. COMDTINST 5510.23 – Coast Guard Classified Information Management Manual. (USCG accounts only).

h. NAG 53 (series) – Keying Standard for Non-Tactical KG-84/KIV-7 Point to Point Circuits (**Only required by shore-based accounts**)

i. NAG 16 (series) – Field Generation and Over-the-air Distribution of tactical Electronic Key. (Required only if the account is involved in OTAT/OTAR operations).

j. NSA Mandatory Modification Verification Guide (MMVG) available only in hardcopy form, through CMIO at (757)444-7051, extension 108.

k. OPNAVINST 2221.5 (series) - Release of COMSEC Material to U.S. Industrial Firms Under Contract to USN. (Required only by those accounts which have an occasion to release COMSEC material to contractors). Available at:
http://www.dtic.mil/whs/directives/links.html

l. SECNAV M5510.36 (series) - Information Security Program Regulation. Available at:
http://www.dtic.mil/whs/directives/links.html

m. SECNAV M5510.30 (series) – DON Personnel Security Program (PSP) Instruction. Available at:
http://www.dtic.mil/whs/directives/links.html

n. OPNAVINST 5530.14 (series) - Physical Security and Loss Prevention. Available at:
http://www.dtic.mil/whs/directives/links.html

o. SECNAVINST 5040.3 (series) - Naval Command Inspection Program. Available at:
http://www.dtic.mil/whs/directives/links.html

~~p. NAVICPINST 2300.4 (series) - Utilization and Disposal of Excess COMSEC Material. Available at:
https://aicpm16.icpmech.navy.mil/kms/navicpdi.nsf~~

AMD-9

~~q. NAVICPINST 5511.24 (series) - Classified Electronic COMSEC Material in the Navy Supply System. Available at:~~

~~https://aicpm16.icpmech.navy.mil/kms/navicpdi.nsf~~

p~~r~~. OPNAVINST 2221.3 (series) Qualifications of Maintenance Personnel (Article 610). Available at: http://www.dtic.mil/whs/directives/links.html

AMD-9

q~~s~~. CJCSI 3260.01 (series) - Joint Policy Governing Positive Control Material Devices. (Required only if account holds SAS material). The most recent version is available by calling J3 at the Chairman of the Joint Chiefs of Staff Office, Commercial: 703-692-6932 or DSN 222-6932.

AMD-9

r~~t~~. SDIP 293 - NATO Cryptographic Instruction. (**Required only if the account holds NATO material**). Available from: http://www.iad.nsa.smil.mil/resources/library/nato/index.cfm

s~~u~~. AMSG 600 – NATO Communications Security Information. (**Required only if the account holds NATO material**).

724. TRANSACTION STATUS LOG:

a. LCMS records and assigns a sequential transaction number (TN) to accounting reports and retains a transaction log of all accounting transactions for the current calendar year and the two previous years. LCMS operators can use the Transaction Status Log to retrieve information about a transaction until the transaction is archived. Archived transactions and related data can be restored by an LCMS operator following the procedures outlined in the EKMS-704(series).

b. Transaction logs will be closed out at the end of each calendar year and retained in accordance with Annex T. **This will be accomplished by drawing a line just below the last line of the TN log, annotating "No further TNs used this year", and the Manager or an Alternate will sign/date the closed out log. For previous year TN logs still required to be on file, they will be annotated in the same manner by the current Manager or Alternate.**

727. COMSEC MATERIAL ACCOUNTING REPORTS:

a. COMSEC Material Accounting Reports (e.g., SF-153s) are used to document the receipt, transfer, destruction, inventory, possession, relief from accountability and generation of COMSEC material. They provide an audit trail for each item of accountable COMSEC material. These reports may be prepared manually or be computer generated.

b. Specific requirements for submitting reports to the COR or NCMS and retention of documentation at the local level are provided in the Articles below that address each particular type of report.

c. These are the most commonly used COR-reportable accounting reports. Other report types including local issue transactions can be found in EKMS 704(series). The various reports, their Tier 1 Transaction Type Number, and a brief description of their general use is reflected below.

(1) Transfer Report Initiating (TRI)/Type 13: Used to document and/or report the movement of COMSEC material between EKMS accounts.

(2) Destruction Report/Type 1: Used to document and/or report the destruction of COMSEC material.

(3) Possession Report/Type 9: Used to bring an item into proper accountability when not received via account-to-account transfer. Examples include; when material is reproduced, following site initialization of a KOK-22A (KP) to bring REINIT1 and NAVREINIT2 CIKS into accountability, etc… Additional uses and information related to Possession Reports can be found in Article 739.

(4) Transfer Report Receipt All (TRRA)/Type 14: Used to document and/or report receipt of COMSEC material when an existing Transfer Report Initiating (TRI/Type 13) exists.

(5) Transfer Report Receipt Exception (TRRE)/Type 15: Used to exclude items not received from a Transfer Report Initiating.

(6) Transfer Report Receipt Individual (TRRI)/Type 16: Used to document and/or report receipt of COMSEC Material when no Transfer Report Initiating exists at the time of receipt. Subsequent submission of the TRI is still required in order for a TRRI to be processed in Common Tier 1.

(7) Relief from Accountability Report/Type 11: Used to remove items from LCMS and accountability to the COR, as applicable when a transfer or destruction report is not on file for the material and also to correct accounting discrepancies unable to be resolved through the use of a conversion report. Use of this report is typically in conjunctions with a COMSEC

Incident report. Additional uses are identified in Article 745.a. Use of this support type requires NCMS approval.

(8) Conversion Report/Type 0: Used to correct Short Title and ALC Code discrepancies or changes. Conversion reports cannot be used to correct serial/reg number discrepancies or to lower the ALC Code for material reflected on the AIS. These type of discrepancies must be resolved with a COR Manager and typically require a Relief from Accountability report to resolve the matter. **Conversion Reports are submitted only when specifically directed by the COR or NCMS.**

(9) Request Inventory/Type 18: Used by the COR to trigger the inventory cycle process. This is also known as a Request for Inventory (RIT).

(10) Inventory Report/Type 6: Used to document and report the physical inventory of COMSEC material.

(11) Inventory Reconciliation Status Transaction (IRST)/ Type 17: Used to report the differences (i.e. discrepancies) between the Tier 1 and Tier 2 databases.

(12) Generation Report/Type 5: Used to document the generation or importation of key.

(13) Cancel Distribution/Type 10: Used to cancel a Transfer Report Initiating (TRI) or Issue Report Initiating and to document/report the cancellation.

d. Reports **must be** submitted electronically via the X.400 Message Server. Timely and accurate submission of accounting reports will ensure that the COR database properly reflects all COMSEC material charged to an EKMS account and prevent possible tracer action.

730. GUIDANCE FOR SUBMITTING REPORTS TO THE COR:

a. Reports that are eligible for submission to the COR via an EKMS transaction must be forwarded via the X.400 Message Server. Submission via any other means requires prior authorization from the COR.

NOTE: Do not forward hardcopy SF-153s for reports that have been submitted electronically unless specifically directed by the COR.

733. TRANSFER INITIATING REPORT (Type 13)

a. **Defined**: A transfer is the movement of COMSEC material, hardcopy or electronic, between two EKMS accounts. There are two types of transfers:

(1) Account-to-Account (Intra-DON) Transfer: The transfer of COMSEC material between two DON EKMS accounts.

(2) Transfer Between Services (Inter-Service): The transfer of COMSEC material between a DON EKMS account and the COMSEC account of another service (e.g., Army or Air Force), agency (e.g., NSA, DACAN, SECAN), department (e.g., State Department), nation, or commercial contractor. **Procedures for transferring CCI *outside DON channels* (i.e., between services/inter-transfers of CCI) are reflected in Article 733.h**.

b. **Transfer Authorization**:

(1) Keying Material and Manuals. The transfer of COMSEC keying material marked or designated CRYPTO(both in physical form and electronic key) and AL Code 1 and AL Code 2 COMSEC manuals must be authorized in accordance with the applicable transfer authorization indicated in this manual or by the Controlling Authority or NCMS. Except as indicated in Article 675, prior authorization is required to transfer keying material marked/designated crypto from the Controlling Authority.

NOTE: The generating account is the CONAUTH for ALC 7 produced at the account level; the CO of the generating account may authorize the transfer per Annex C.

(a) CONAUTHs are listed in the SCMR or on the material itself (e.g., Letter of Promulgation for manuals) or on SIPRNET at www.jfcom.smil.mil/jcmo/homepage.ncf.

(b) Any transfer that constitutes a temporary or permanent modification to the authorized holdings of an account must be handled in accordance with Chapter 6.

(2) COMSEC Equipment and Related Devices. **With exception to KGV-68Bs**, the transfer of crypto equipment and related devices must be authorized in accordance with Chapter 6. See Article 770 regarding the transfer of KGV-68Bs.

c. **Material Transferred Electronically Between DON**

Accounts: **No hard copy documentation is required** for material transferred electronically between DON EKMS accounts via the message server. LCMS maintains the required documentation using transaction Type 13/TRI.

d. **Physical Transfer of Material Between DON Accounts**:

(1) The physical transfer of material includes all material transferred other than electronically (i.e., via a means other than the Message Server or over-the-air transfer (OTAT/OTAD)).

(2) The physical transfer of AL Code 1, 2, or 4 material between DON accounts requires a hard copy TRI SF-153. The account will reconcile for the material with the electronic TRI, if provided; however, effective **with AMD-7**, the hard copy SF-153 will be completed and signed by two account personnel in accordance with Annex U and retained in accordance with Annex T.

NOTE: If material was receipted for with exceptions, a Transfer Report Receipt Exception Report(TRRE) must be sent to the COR and the COR notified out-of-band of the accounting transaction information. Do not send the TRRE to the originating account; contact the account and notify them of the discrepancy out-of-band. The COR Account Manager will provide additional guidance to both the originating and receiving accounts.

(3) The transfer of AL Code 4 material between DON accounts will use the local custody issue procedures outlined in Article 769.

e. **Reconciling the Transfer/Report:** Two functions are available to reconcile transactions after the originator receives the TRI from the recipient; each function is discussed below:

(1) Reconcile Electronic Receipt: This is the preferred method for reconciling receipts and is used when a TRI (Type 13) electronic distribution report was used to document the transfer. EKMS/COMSEC Accounts which begin with 0, 1, 2, 3, 5, 6, 7 and 88 and 89 will provide electronic TRIs for all shipments; therefore, a TRRA is the preferred response when received. If an electronic TRI has not been received from the originating account, contact the account and request one. If an electronic TRI was received by the receiving account only an electronic TRRA or TRRE may be used to receipt for the shipment.

Use of any other accounting report to document receipt will require prior authorization from the COR, since it will cause accounting options otherwise

(2) Reconcile Hard Copy Receipt: This function is used when a hard copy TRR SF-153 was used to document the transfer and an electronic TRI has not been received from the recipient and the account needs to close-out the transaction. EKMS/COMSEC Accounts which begin with 87 are normally contractor (non-automated) accounts and may only provide hard copy transfer reports SF-153. Transactions received from these accounts will be receipted for using a Transfer Receipt Report Individual. The hard copy (signed) receipt will be mailed to the originator of the shipment with an electronic copy sent to the COR via the Message Server. If the "Reconcile Hard Copy Receipt" function is used and subsequently an electronic TRI is received, the electronic TRI will be irreconcilable and unable to be removed from the LCMS desktop. Do not process this TRI using a TRRE without prior authorization from NCMS.

f. **Documentation Requirements**:

(1) A hardcopy TRI SF-153 Transfer Report must be prepared and forwarded with all physical shipments to facilitate proper forwarding in the event that the package is misrouted. The transferring account must also send an electronic copy of the TRI to the receiving account via X.400.

(2) Account-to-Account Transfer Between a DON Account and a non-DON Account (Inter-service Transfer): For all DON to non-DON shipments of physical material ***excluding CCIs***, transferring accounts must do the following (documentation requirements for *inter-service transfers of CCIs* are in Article 733.h below.

(a) Prepare and send the TRI SF-153 electronically to the COR and the receiving account unless the recipient is an 87 account (contractor). For contractor transfers, transfers and receipts will generally be via hard copy documentation.

(b) Forward the original TRI SF-153 with the shipment and retain a copy in transferring command's files pending acknowledgement of receipt by the recipient.

(3) Account-to-Account Transfer between Two DON Accounts (Intra-Service Transfer).

(a) AL Code 1, 2 or 6 material: Transferring accounts will prepare a TRI SF- 153 original and one copy. The original will be forwarded with the shipment and the copy will be retained in the transferring command's files pending acknowledgement of receipt by the recipient. The TRI must also be sent electronically to the COR and the receiving account.

(b) AL Code 4 material transferred to a VDLS, PMHS, or CMIO: Transferring accounts will prepare a TRI SF- 153 original to be forwarded with the shipment and one copy to be retained pending acknowledgement of receipt by recipient. Recipient will verify TRI SF-153 against shipment contents and then receipt to the COR electronically using the TRR EKMS transaction.

(c) AL Code 4 material transferred to all other DON accounts: Transferring accounts will prepare an original and one copy of a TRI SF-153 and use the local custody issue procedures in Article 769.

g. **Reporting Requirements**:

(1) Regardless of service affiliation, the physical transfer of all AL Code 1, 2, or 6 COMSEC material involving a DON EKMS accounts must be reported to the COR via a TRI EKMS Transaction prepared by the account transferring the material.

NOTE: See Article 742 **for receipt procedures].**

(2) The transfer of AL Code 4 COMSEC material to a VDLS, PMHS, CMIO, or a non-DON account must also be reported to the COR electronically.

h. **Inter-Service Transfer of CCI**:

(1) DON EKMS policy mandates that its CCI will be continuously accounted for *within* the CMCS. U.S. Air Force and Army control their CCI *outside* of the CMCS, in their respective requisitioning and issue systems (e.g., MILSTRIP). This difference in how the services account for CCI necessitated that unique transfer and receipt procedures be developed. These procedures, unique to CCI transactions involving Air Force and Army organizations, are outlined in this Article.

(2) LCMS will only accept valid EKMS account numbers in the From/To Account block of transaction reports. Defense Activity Address Code (DODAAC) account numbers cannot be

used as a substitute for EKMS account numbers on transaction reports. DON EKMS managers must strictly adhere with the below procedures to properly transfer and/or receive CCI from Air Force and Army organizations.

(3) **Transferring CCI to Air Force and Army -** Follow these procedures in the order indicated:

(a) Obtain transfer authorization from NCMS (N3).

(b) Contact the organization that will be gaining the CCI to obtain the name and telephone number of the receiving accountable office and the organization's complete shipping address. If obtaining the information proves difficult, contact the appropriate agency that follows:

U.S. Air Force Cryptologic Systems Group,
Lackland AFB, TX
(DSN 969-4805)

U.S. Army Communication Security Logistics
Activity (USACSLA),
Fort Huachuca, AZ 85613-7041
Customer Service Center
(1-877-896-8094 or DSN 879-9900)

(c) Telephone the receiving accountable officer and inform him/her of the impending CCI shipment.

(d) Generate and submit a SF-153 Relief from Accountability Report electronically to the COR, annotating in the remarks section of the report the authorization for the transfer.

(e) Use a DD form 1348-1, DD FORM 1149, DD Form 250 or locally prepared transfer/receipt to document the transfer to the Air Force or Army organization and include that document in the shipment.

(4) **Receiving CCI from Air Force and Army --** Upon receipt of the CCI:

(a) Inventory shipment contents against the enclosed documentation. Then prepare and submit a SF-153 Possession Report electronically to the COR. Cite this article or other authorization in the remarks section of the report any documentation or authorization for the receipt.

(b) Receipt to the Air Force or Army originator using whatever documentation was enclosed in the shipment.

NOTE: Transfers of CCIs from other departments and Agencies through other than CMCS channels may be received on various types of voucher documents, including the DD 1348-1, DD 1149, DD 250 or other similar forms prescribed by the shipper's service or agency regulation.

736. DESTRUCTION REPORT (Type 1)

a. **General**:

(1) Except in cases of extreme emergency (e.g., enemy attack, civil uprising, or natural disaster, or terrorism), COMSEC material must always be destroyed by two appropriately cleared and authorized persons.

(2) The destruction report must be completed immediately after the material is destroyed.

(3) Document destruction of individual segments (i.e., tape segments, days, pages, etc.) of COMSEC material using the forms and guidance contained in Figure 7-1, 7-2, or 7-3, as appropriate. Destruction of entire editions will be documented on the SF-153 using the guidance contained in Annex U, as appropriate.

(4) Destruction of other hard copy COMSEC and electronic COMSEC material will be completed and documented in accordance with Article 540.

b. **Destruction Documentation and Reporting Requirements**: Consolidated destruction reports must be submitted to the COR.

(1) Reportable Destruction Reports: At a minimum of monthly or sooner if directed, an account must report destruction of AL Code 1, 2, and 6 material to the COR and on these occasions:

(a) When the material is either regularly or irregularly superseded on its supersession date,

(b) Whenever regularly **or** irregularly superseded material is destroyed outside its authorized supersession date (e.g., material is destroyed prematurely or is destroyed as the result of an emergency supersession),

(c) When directed by the COR or NCMS in the process of disestablishing an account,

(d) When local destruction of obsolete AL Code 1 or 2 equipment is authorized by NCMS, and

(e) On any other special occasions as determined by the COR or NCMS.

(2) Local Destruction Records/Reports:

(a) The destruction of regularly superseding COMSEC material will be documented and retained locally using a SF-153, the LCMS destruction report, or locally prepared equivalent form (e.g., CMS 25). Annex U contains guidance for preparing the SF-153 local destruction document.

(b) *Whenever local destruction records are generated manually (outside of LCMS):* Local destruction records must be completed to document the destruction of all TOP SECRET and SECRET material and will be retained in accordance with Annex T. See single exception to this documentation policy in Article 540.c.(3)(a).

NOTE: This is only authorized for detachments or instances where the EKMS Manager cannot generate and provide the destruction report to the LE from LCMS as described above. If necessary for a LE to create a SF-153 for recording destruction outside LCMS, the EKMS Manager will generate and attach the LCMS destruction document to the one signed/submitted by the LE.

(c) *When local destruction records are generated in LCMS:* Local destruction records must be completed to document the destruction of all TOP SECRET, SECRET, and CONFIDENTIAL material and will be retained locally in accordance with Annex T. See single exception to this documentation policy in Article 540.c.(3)(a).

NOTE: The requirement to document destruction of Confidential material in LCMS is system-driven, not policy driven. When using LCMS, local destruction records for Confidential material must be completed; otherwise, the Confidential material will remain on the LCMS AIS.

(d) Local destruction records are mandatory for all

AL Code 1, 2, and 6 COMSEC material, regardless of classification.

(e) Local destruction records are optional for AL Code 4 and 7 COMSEC material classified CONFIDENTIAL and below, regardless of CRYPTO markings.

> **NOTE: Copies or local destruction records (CMS 25, SF-153s (working copies), etc… will be forwarded to the EKMS Manager. Effective with AMD-7, CMS-25s and working copies working copies of destruction reports (SF-153s) will be retained in accordance with Annex T unless longer retention is mandated by local policy.**

(3) LCMS provides the interface for the operator to direct the destruction of locally held electronic key, request and confirm destruction of material by a non-LMD account or LE, report destruction to a superior account, and process electronic destruction reports from an account. See Article 792 and Chapter 4 of EKMS 704 (series) for guidance in destroying electronic key.

739. POSSESSION REPORT:

An SF-153 Possession Report is used to return AL Code 1 or 2 COMSEC material to proper accountability controls, to report the reproduction of AL Code 1 or 2 COMSEC material, to bring items into accountability that were received via Inter-Service transfers, and to bring back into accountability an item which was removed to correct a discrepancy not able to be resolved through the use of a Conversion Report. Justification and/or authorization, where applicable must be included on possession reports.

A Possession Report must be submitted for a whole edition, complete short title, or separately accountable end item of AL Code 1 or 2 COMSEC material on the following occasions:

a. When AL Code 1 or 2 COMSEC material is reproduced for other than local use. See Article 781 for guidance on reproducing COMSEC material.

b. When a KOK-22 (KP) is site initialized and the REINIT1 and NAVREINT2 CIKS are created. Although these items are ALC1 and ALC4, respectively, they must be possessed to bring them into accountability as described in Article 1185.

c. Material is received via an Inter-Service transfer as discussed in Article 733.h.

d. When AL Code 1 or 2 material comes into the possession of an EKMS account by other than a properly documented transfer or receipt (e.g., no SF-153 and originator unknown).

e. When AL Code 1 or 2 material previously charged to the account is found and documentation exists to show that the material was transferred or lost, and is no longer reflected on the A/I Summary.

> **NOTE: Items described in 739.a – 739.c do not require reporting as a COMSEC Incident or NCMS approval to possess these items. Items 739.d and 739.e require submission of a COMSEC Material Incident Report in accordance with Article 945. Possession reports for AL1, 2 and 6 material must be submitted to the COR to ensure the material is properly charged to the account.**

f. Do not submit a SF-153 Possession Report whenever a whole edition, complete short title, or separately accountable AL Code 1 or 2 material is found that was documented as destroyed but follow these instructions:

(1) Report the finding of the material as a PHYSICAL incident in accordance with Article 945.

(2) If the material is authorized for destruction, destroy it and document the actual destruction locally. Indicate in the report of the incident that the found material was destroyed.

(3) If the found material is not authorized for destruction (e.g. found material is equipment or future key that was previously reported as "prematurely" destroyed), request disposition instructions in the incident report.

g. Do **not** submit a Possession Report for AL Code 1 or 2 COMSEC material that is properly documented as charged to the account but is found outside of proper storage. This situation will require submission of a COMSEC Material Incident Report in accordance with Article 945. Within LCMS, the material must be flagged as “pending investigation” until the incident report has been resolved. Follow the procedures outlined in EKMS 704, Chapter 4.

h. Possession reports will not be used as a substitute for a receipt unless except as discussed in article 733.h without authorization by NCMS.

740. GENERATION REPORT (Type 5):

LCMS provides for the automatic creation of both COR Reportable and Local (Non-Reportable) Generation Reports.

a. Reportable Generation Report: This report is created and must be submitted to the COR whenever the following occurs:

(1) AL Code 6 material is generated by the account.

Note: Accounts will not generate ALC-6 or import ALC-1 (physical material) into the LMD/KP environment without prior approval from the COR or Service Authority.

(2) AL Code 1 material is imported in the LMD/KP (i.e., AL Code 1 key tape is converted to electronic form using a KOI-18 and loaded into an electronic storage device (ESD), and subsequently imported into the LMD/KP or loaded directly into the LMD/KP environment from a KOI-18). (Whenever AL Code 1 material is imported in the LMD/KP, it is automatically assigned AL Code 6.)

(3) AL Code 6 material (stored in an ESD) is imported in the LMD/KP.

NOTES: 1. If authorized to import ALC-1 key into the LMD/KP, follow the procedures for "importing" contained in EKMS 704, Chapter 4 and submit the Generation Report electronically to the COR. The generating COMSEC account must send a Free Format Text (FFT) transaction (Type 700) to the COR providing all other attributes for the key as displayed in LCMS following importation and/or generation. The additional information will enable the COR to enter all relevant information in the COR data base that pertains to the imported key and that is not contained in the Generation Report.

2. See Article 781 for guidance on AL Code 1 key imported in the LMD/KP for transfer *outside* the command, and for restrictions on importing/reproducing AL Code 1 key.

3. Commands cannot arbitrarily decide to convert

their entire key tape holdings to electronic form and import them in the LMD/KP to lessen/simplify handling and storage requirements without CONAUTH approval.

4. Timely and accurate submission of accounting reports will ensure that the COR data base properly reflects all COMSEC material charged to an account.

b. Local (Non-Reportable) Generation Report: This report is created whenever the following occurs:

(1) AL Code 7 material is generated by the account.

(2) AL Code 4 material is imported in the LMD/KP (i.e., AL Code 4 key tape is converted to electronic form using a KOI-18 and loaded into an ESD and subsequently imported in the LMD/KP).

(3) AL Code 7 material (stored in a ESD, for example) is imported in the LMD/KP.

(4) Generation reports for ALC 7 material must be retained locally in accordance with Annex T. Do not submit Generation Reports for ALC 7 material to the COR.

c. Signature Requirements: Generation reports will be signed by three personnel as outlined in Annex U.

741. CANCELLATION REPORT (Type 10):

LCMS provides an interface for the operator to cancel a TRI or Issue Report Initiating (IRI) of material not yet distributed. Examples of when one would create a Cancel Distribution Transaction (CDT) include: A floppy disk containing the transaction was destroyed, physical material was destroyed in transit, or a transaction was prepared and circumstances cancelled the need for the material to be distributed. LCMS also enables the operator to process a received CDT from the COR, a parent account, or another LMD-equipped account. There are two types of Cancellation Reports: Cancel Distribution Local and Cancel Distribution Forwarded. Both are discussed briefly below and also in detail in Chapter 4 of the LMD/KP Operator's Manual (EKMS 704 (series)).

a. Cancel Distribution Local: This report is created locally when the TRI or IRI was created but the material was not transferred or issued and the TRI/IRI was not wrapped. The processing of this report returns the physical material to the account's AIS with a status of "on hand". Copy-controlled electronic key is recorded as "destroyed". This transaction is addressed to the local account and is NOT forwarded to the COR.

b. Cancel Distribution Forward: This report is used to cancel a shipment which has already been shipped from the account or prepared for shipment but not sent when the TRI was forwarded ahead of the shipment. It is created and sent to both the COR and the account the transaction was sent to. This transaction updates the LCMS database as follows:

(1) Physical Material: Is returned to the account's AIS with a status of "Pending Investigation". Before this material can be used by the account, the Pending Investigation flag must be removed and a Possession Report created which will change the status of the material to "on hand". Use this article as authorization to prepare the Possession Report, do not forward this report to the COR.

(2) Electronic Key: Is returned to the account's AIS with a status of "Pending Investigation". Because the key was encrypted in the credentials of the receiving account at the time of distribution, it cannot be returned to stock in the originator's account. A Relief from Accountability report must be created to remove the material from the account's AIS. Use this article as authorization to prepare the Relief from Accountability report, do not forward this report to the COR.

Both forms of the Cancel Distribution Transaction (CDT) are discussed in more detail in Chapter 4 of the LMD/KP Operator's Manual (EKMS 704 (series)).

742. <u>RECEIPT REPORT</u>:

a. **<u>Reporting Criteria</u>**: Except as indicated in subparagraphs (b) - (d) below, all receipts must be reported to the originator of the shipment and the COR via the X.400 message server using one of the below described EKMS transactions. Hard copy receipts are not required or desired by the COR or CMIO for material receipted for electronically via the message server.

1. Transfer Receipt Report ALL (<u>TRRA)/Type 14</u>. This transaction is used when all material in the shipment has been received and accounted for.

2. Transfer Receipt Report Exception (<u>TRRE)/Type 15</u>. This transaction is used when all material on the TRI SF-153 cannot

be accounted for (i.e., missing item) in the shipment.

3. Transfer Receipt Report Individual (TRRI)/Type 16. This transaction allows material to be receipted for in LCMS when no TRI has been received.

NOTE: If EKMS Managers reconcile for material with the electronic SF-153 without any discrepancies but choose to retain the printed copy of the SF-153 receipt, the SF-153 will be signed, completed and retained in accordance with Annex T.

b. **Reporting Receipt of ALC-4 and ALC-7**:

1. Initial receipt of ALC-4 or ALC-7 material from the CMIO or the USNDA will be reported as indicated above.

2. The receipt of ALC-4 or ALC-7 material from other DON accounts will be reported to the originator of the shipment or BET, as applicable. Do not report receipt of ALC-4 or ALC-7 material received from other Tier-2 accounts to the COR.

c. **Reporting Receipt of CCI from Army or Air Force Accounts**: See Article 733.h for proper procedures related to inter-service transfers and required actions to bring CCI from the Army or Air Force into CMCS accountability.

d. **Reporting Receipt of Physical Material from 87XXXX (Contractor Accounts)**: If the 87XXXX account is LMD or LMD/KP equipped, (as verifiable through CAD data in the X.500 directory service) receipt for the material as discussed in subparagraph (a) above; if not, create a TRRI and electronically report receipt to the COR via X.400. A signed hard copy with the date of report and incoming TN number must be returned to the address in Block (2) of the transfer SF-153.

e. **Timeframe for Reporting Receipt**:

(1) A receipt must be forwarded **within 96 hours** after receiving electronic or hardcopy COMSEC material.

(2) The 96 hour clock begins either from the time the BET and TRI enters the account's LMD/KP via the message server (electronically), from the time picked up over-the-counter from a VDLS component (e.g., DCS), or from the time the material is received at the command.

NOTE: In those instances where the shipments are staggered and reflected on a single transfer report the 96 hour rule begins when the entire shipment is received.

(3) If emission control (EMCON) or MINIMIZE is in effect, which precludes receipt via the message server, report receipt via email, facsimile or mail.

(4) Failure to submit receipts within 96 hours must be documented in accordance with Article 1005.a.

f. **Discrepancies**:

(1) Report inner package damage, evidence of tampering, or incorrect shipping methods in accordance with Chapter 9.

(2) Report contents discrepancies (i.e., material in the shipment does not correspond with the material listed on the SF-153) in accordance with Article 754.c.

(3) Report discrepancies in the material itself (e.g., page check errors) in accordance with Annex V.

g. **Bad Bulk-Encrypted Transaction (BET) Procedures**:

(1) Expired FIREFLY credentials is the most common reason an account cannot reconcile for received BETs.

(2) Dependent upon the originator and recipient of the BET, different processes are defined for resolution of these situations.

(3) EKMS Managers must report receipt of corrupt BETs within 96 hours of downloading the BET. Failure to report the receipt of corrupt BETs within 96 hours of downloading must be documented in accordance with Article 1005.a.

(4) Specific procedures for addressing receipt of BETs which cannot be processed can be found in the table below.

If the Bad BET Originator is…	**Preferred Reporting Method**	**Alternate Reporting Method**
880091/Central Facility Fort Meade and the Transaction Number is less than 80000	Send DMS or AMHS Message to: AMHS- DIRNSA FT GEORGE G MEADE MD DMS- NSA/CSS//I31// Include on all: • Originating Account (should be 880091) • Date of BET • Transaction Identification Number • Receiving Account • Error Message (Full text of error message displayed to the Tier 2 operator) • Replacement Key Required – Yes or No (unless otherwise specified, all non-superseded KEYMAT will be resent automatically) • Any other pertinent information	Send an UNCLASSIFIED PKI signed email with Irreconcilable BET form to: BadBET@radium.ncsc.mil If no response is received in 2 days, call: (240)373-1480 Include Command PLA in addition to Information listed in Preferred Reporting Method column
880103/Central Facility Finksburg and transaction number is 80000 or greater	Send UNCLASSIFIED PKI signed email with Irreconcilable BET form to: centralfac@radium.ncsc.mil	FAX UNCLASSIFED Irreconcilable BET form to: (410)517-3321 or DSN 238-4321
Unable to determine NSA source or Require Special Assistance	Contact NSA Key Support Center (KSC): Commercial – 1-(800)635-5689 Email - centralfac@radium.ncsc.mil	
5A8240 or 5A8242(Tier 1 Fort Huachuca)	Send an UNCLASSIFIED PKI signed email with Irreconcilable BET form to: csla.list.huactier1-5a8240-badbet@mail.mil	Contact Fort Huachuca Help Desk: (520)538-9900 or DSN 879-9900
616502(Tier 1 San Antonio)	Send UNCLASSIFIED PKI signed email with Irreconcilable BET form to: AFLCMC/HNCD.TIER1.OPS@us.AF.MIL	Contact San Antonio Help Desk: (210)925-1789 or DSN 945-1789
Another Tier 2 account	Any Common Communication Method	

Note: The information required in the irreconcilable BET form is the same as that indicated in the first row above. This same information can be supplied using one of the above communication methods without the need for a separate form. Any information omitted however, will result in either a delayed action or rejection of the request.

743. TRACER ACTIONS FOR OVERDUE RECEIPTS:

a. Tracers are generated by originators of COMSEC material transfers at specified time intervals to notify intended recipients of overdue receipts. Before initiating tracer action, originators will allow for normal delivery and return mail time. Include the respective COR, DIR TIER1 SAN ANTONIO TX **or** CSLA TIER1 and NCMS//N3// as an INFO addressee on all tracer actions.

b. Tracers will be sent via the X.400 at designated time periods and may originate from the originator, Tier 1 or both.

NOTE: Regardless of the originator of the shipment, Tier 1 will initiate a tracer for any outstanding TRI for which a corresponding TRR has not been received and processed by the COR.

c. If the EKMS Manager has not received a shipment for which a tracer notice has been received, the EKMS Manager will notify the originator of the shipment immediately.

d. The three most common tracer report intervals are:

(1) FIRST TRACER is sent 30 days from the date of a shipment. EKMS Managers must respond consistent with a ROUTINE precedence action GENSER or DMS signed message.

(2) SECOND TRACER is sent 40 days from the date of a shipment. EKMS Managers must respond consistent with a PRIORITY precedence action GENSER or DMS signed message.

(3) THIRD TRACER is sent 50 days from the date of shipment. EKMS Managers must respond consistent with an IMMEDIATE precedence action GENSER or DMS signed message.

e. Shipment originators that do not receive either a communication or a receipt from the intended recipient within 60 days of the date of the first tracer action will generate a COMSEC Material incident report ("Physical Incident") per Article 945.e . The shipment originator will include the intended recipient command as an INFO addressee and identify the intended recipient command in the report's narrative as failing to respond to repeated tracer actions.

f. Tracers may also be sent by the COR, NCMS, NSA, or via automated notification process from Common Tier 1 if receipt is not received for a COMSEC material transfer they originated. The same action is required by the EKMS Manager upon receipt of a tracer from the COR, NCMS, or NSA. The aforementioned entities may not follow exactly the time intervals but may deviate from them as individual circumstances may require.

NOTE: Failure to respond to a final tracer notice from the Central Facility for Modern Key may result in the key being marked as compromised and placed on the "Compromised Key List" (CKL).

744. RECONCILIATION:

a. Reconciliation is the process through which received accountable material is added to the local account's data base. A distribution report (electronic TRI or hard copy SF-153) accompanies each shipment of material and contains information about the contents, source, and destination of the shipment. After the receiving account receives and processes the distribution report, it generates a receipt for the originating account. Reconciliation of the receipt at the sending account relieves the originator from accountability for the items contained in the associated distribution report. An automated capability has also been provided to return physical material back to the account from a LE.

b. Distribution receipts are generated by accounts that receive accountable material to notify the originating element that the destination element accepts accountability for the distributed material.

c. See the LMD/KP Operator's Manual (EKMS 704 (series)) for a more detailed explanation of the many variations and uses of the Reconciliation Report (e.g., Reconcile Physical Material Hard Copy Report, Reconcile Electronic Package, Reconcile Hard Copy Receipt, Reconcile Electronic Receipt, etc.).

NOTE: To minimize accounting errors, when provided by the originator, EKMS Managers will reconcile for all material using the electronic version of the SF-153.

745. RELIEF FROM ACCOUNTABILITY REPORT:

a. A Relief from Accountability Report is submitted to the COR whenever a whole edition, complete short title, or separately accountable end item of AL Code 1, 2 or 6 material is missing and no documentation exists which indicates that the item was either transferred or destroyed. It is also submitted to document and report missile firings (see Annex AB), to correct accounting errors which cannot be corrected with a Conversion Report, to change a material "type," and when performing an inter-service/agency transfer of CCI, per Article 733.h. Except for instances covered in Articles 733.h, 741.b.2 and Annex AB, use of this report **must be** authorized by either the COR or the SERVAUTH (NCMS).

b. In the case of missing material, the EKMS account charged with the material must submit a COMSEC Material Incident Report in accordance with Chapter 9, in addition to the SF-153 Relief from Accountability Report. Within LCMS, the material must be flagged and removed from the A/I Summary per EKMS 704, Chapter 4 procedures.

c. SF-153 Relief from Accountability reports require three signatures, the EKMS Manager (or Alternate), a witness and the Commanding Officer and will be submitted to the COR via the Message Server. The original Relief from Accountability report will be retained in accordance with Annex T. Instructions on completing this report are found in Annex U.

748. CONVERSION REPORT:

a. An SF-153 Conversion Report is used to correct Short Title and ALC Code discrepancies or changes. Conversion reports cannot be used to correct serial/reg number discrepancies, edition discrepancies or to lower the AL Code for material reflected on the AIS.

b. This report consolidates two separate reports into a single document. One which was used to delete a short title/accounting data from account records and the other to add the correct data into account records.

c. Conversion reports are only submitted to the COR when specifically directed to do so by the COR.

751. RECEIVING AND OPENING COMSEC MATERIAL SHIPMENTS:

a. **General**: Most COMSEC material is shipped from the USNDA, CMIO and other accounts via the Defense Courier Service (DCS). DCS contacts are located at: http://www.transcom.mil/dcd. **Account managers must accept and receipt for material shipped to the account. Refusal to accept**

material is prohibited and may impact unit readiness, results in excess shipping costs and could jeopardize the security and accountability of the material.

b. **USTRANSCOM FORM 10**: An up-to-date USTRANSCOM FORM 10 is required to pick-up material from DCS. Instructions for completing the Form-10 are available from servicing DCS stations or online at the above URL under the customer service tab.

c. **CMS Form 1**: An up-to-date CMS Form 1 is required to be on file at the CMIO for pick-ups or turn-in of material. This form must be updated in accordance with Chapter 6.

d. **Summary of processing steps upon opening COMSEC material**:

(1) Inspect both the inner and outer wrapper for signs of tampering.
(2) Open the shipment.
(3) Inventory the contents against the enclosed SF-153.
(4) Conduct a Protective Packaging inspection.
(5) Conduct page checks as required by Annex W.
(6) Apply status information (less equipment).
(7) Reconcile for the material in LCMS.
(8) Properly store the material.

e. **Who May Open COMSEC Material Shipments**:

(1) All COMSEC **keying material** shipments must be opened by **two** persons, one of whom must be the EKMS Manager or Alternate. The other person may be any properly cleared and authorized EKMS witness. The presence of two persons is necessary in the event that TPI is required (i.e., the shipment contains Top Secret hard copy).

(2) Upon verification that the shipment does not contain TPI material, the shipment can then be processed by one individual. Although two people are not required, it is strongly recommended for ease of verifying the contents against the enclosed SF-153.

NOTE: Personnel other than EKMS Managers are authorized authorized to assist Managers (or Alternates) in opening and processing material shipments, providing they are properly cleared and are under the direct supervision of the EKMS Manager (or Alternate).

(3) Opening of a Shipment by Other Than the Intended Account:

(a) If a COMSEC material shipment belonging to another account is inadvertently opened by an EKMS Manager or Alternate, the contents of the shipment must be inventoried immediately.

(b) The package must be resealed immediately and promptly forwarded to the proper command. The body of the enclosed SF-153 must be annotated as follows:

"NOTE: Package number (____) was opened inadvertently (date) by (name of command), account number (______). The contents were inventoried (date) and the shipment sealed immediately. Signed: (signature of EKMS Manager or Alternate of command that inadvertently opened the package). Witnessed: (signature of witness)."

(c) If the TRI SF-153 Transfer Report in the inadvertently opened package is incorrect or missing, use the procedures in the following paragraphs to correct or prepare a TRI SF- 153. If a TRI SF-153 must be prepared, ensure the above note is placed in the body of the SF-153.

NOTE: All personnel who regularly receive and process mail and packages addressed to the command (e.g., mailroom or administrative personnel) must be advised to not open packages specifically marked for the account or EKMS Manager.

754. REQUIRED ACTIONS UPON RECEIPT OF COMSEC MATERIAL:

a. **STEP I**: Inspect packages for tampering: Upon receipt of a COMSEC material shipment, immediately inspect the inner shipping wrapper for damage or evidence of tampering. If evidence of either is found, retain the wrappings and submit a COMSEC Incident Report in accordance with Chapter 9. For assistance in inspecting protectively packaged COMSEC material (e.g., canisters), account personnel are encouraged to contact their servicing ~~Advice & Assistance (A&A)~~COR Audit Team. These teams provide comprehensive instruction on inspecting the various tamper-evident packaging technologies and will, upon request, provide copies of the NSA's library of Protective Technologies Pamphlets.

AMD-9

b. **STEP II**: Inventory the Contents: Inventory the contents of the shipment against the enclosed SF-153 Transfer Report and comply with the applicable step below:

(1) Shipment contents do not correspond exactly to SF 153 Material Listings: Follow the instructions in Step III.

(2) No SF-153 enclosed, but originator known: Follow the instructions in Step IV.

(3) No SF-153 enclosed and originator **NOT** known: Follow the instructions in Step V.

(4) SF-153 enclosed, contents correspond exactly: Follow the instructions in Step VI.

c. **STEP III**: Contents Discrepancy: Shipment contents do not correspond exactly to SF-153 Material Listings.

(1) Correct the SF-153 listing to reflect exactly the material in the package, and initial all corrections (EKMS Manager or Alternate and a properly cleared and authorized individual).

(2) Report the nature of the discrepancies to the originator of the shipment and the servicing PT1S via message server using the TRRE transaction.

AMD-9

(3) Inspect protectively packaged keying material upon receipt in accordance with the applicable Protective Technologies Pamphlet. Commands are encouraged to contact their servicing ~~Advice and Assistance (A&A)~~COR Audit team for instruction on inspecting tamper-evident technologies and for copies of the complete library of Protective Technologies Pamphlets. Protective Technology products are also available at: www.iad.smil.mil/iaservices/protective_tech/index.cfm

(4) Follow the instructions in Step VI to report the receipt.

d. **STEP IV**: No SF-153 enclosed, but originator known:

(1) Ensure the TRI SF-153 has not been transmitted electronically. If the TRI is located on message server, print a copy and verify the shipment contents against the TRI. If the TRI cannot be located, forward a message to the originator listing the short titles and accounting data of the contents and request confirmation of the shipment contents. Also request an

outgoing TN and date to complete the TRI. Include the COR and NCMS//N3// as an information addressee on these reports.

> **NOTE: If a message cannot be used, forward a facsimile or letter to the originator, COR, and NCMS//N3// listing the short titles and accounting data of the contents.**

(2) Retain all packaging material and shipping containers until the discrepancy is resolved.

(3) Enter the material on the (A/I) summary.

(4) After verification of the contents of the shipment and receipt of an outgoing TN from the originator, prepare a TRRA and report receipt of the shipment in accordance with Article 742.

(5) If verification from the originator of the shipment is not received within 7 days, follow the procedures in Step V.

e. **STEP V**: No SF-153 enclosed and originator **NOT** known:

(1) Forward a message, facsimile, or letter to the COR and NCMS//N3// stating the circumstances and listing the short titles and accounting data of the contents.

(2) Retain all packaging material and shipping containers until the discrepancy is resolved.

(3) Submit a SF-153 Possession Report in accordance with Article 739 and Annex T.

f. **STEP VI**: SF-153 enclosed and contents correspond exactly: Complete the TRI SF-153 and submit a TRRA in accordance with Article 742.

755. LCMS ACCOUNT RECONCILIATION FOR MATERIAL RECEIVED:

LCMS supports reconciling of electronic and hard copy receipts for material received and material distributed. There are three functions available for reconciling received material:

a. **Reconcile Physical Material Electronic Report**: The preferred method for reconciling for material. This method reduces or eliminates manual data entry errors and must be used when the originator provides an electronic version of the SF-153 used to document the transfer.

b. **Reconcile Physical Material Hard Copy Report**: The use of a hard copy SF-153 to reconcile for material is **only authorized when the originator does not provide an electronic version of the SF-153.**

c. **Reconcile Electronic Package**: Select this function to receipt for electronic keying material sent from an EKMS-capable account with an electronic SF-153.

757. CONDUCTING PAGE CHECKS AND VERIFYING COMPLETENESS OF COMSEC MATERIAL:

NOTE: For COMSEC equipment/host devices which contain embedded crypto/CCIs, see Article 758.

a. **Purpose of Page checks**: Page checks are conducted to ensure the completeness of COMSEC material (except for protectively packaged material) and COMSEC related material.

NOTE: Material that is protectively packaged must NOT be opened and removed to facilitate page checking for completeness. The protective packaging is intended to remain intact on the material until the material must be removed for issue/use.

b. **Verify Before Installation/Use**: COMSEC equipment, related devices, and components must be verified for completeness well in advance of their installation/use so that there is ample time to obtain replacement equipment or parts, if required.

c. **Establish Internal Procedures**: The Manager must establish internal procedures to ensure that all COMSEC material received by an account is page checked and/or verified for completeness in accordance with this manual.

d. **Certify Completed Page checks**: Certification of completed page checks for COMSEC publications and keying material must be recorded on the Record of Page checks (ROPs) page for the material, or on the front cover for material having no ROPs page.

e. **Page check Requirements**: Minimum page check requirements for all COMSEC material are contained in Annex W. Some requirements are repeated here for emphasis and because of the unique procedures that must be followed.

(1) Do not open sealed crates containing COMSEC equipment or sealed/resealed packages of keying material for the sole purpose of complying with the page check upon receipt requirement.

(2) Page check unsealed COMSEC keying material upon initial receipt, upon transfer, during all account inventories, during daily watch-to-watch inventory, and prior to destruction.

(3) Unsealed daily changing call signs or code books Communication Electronic Operating Instructions (CEOI) (e.g., AKAI, AKAU, AMSH) are exempt from the requirement to page check each copy upon initial receipt. Recipients need only check one or two copies of each new edition upon receipt to ensure page and print continuity.

(4) To reduce the possibility of a COMSEC incident as a result of a missing page to a classified COMSEC publication, all classified COMSEC-related publications issued to LEs including but not limited to KAMs, KAOs, AKACs, AKAIs, AMSH, etc. will be page checked during watch to watch inventories or when a container is opened if held by a non-watch environment. These items will be indicated by an asterisk (*) on watch-to-watch inventories to reflect that a page check is required. Due to space limitations on the cover or ROP page, the signing of the inventories at the LE level will certify the page check was properly conducted with no discrepancies.

f. **Procedures**: Each item of printed COMSEC material contains a List of Effective Pages (LOEP), either on a separate page or on the front cover of the material. This list indicates which pages should be in the publication and identifies the status of each page (i.e., an original page or a specific amendment number page).

NOTE: Annex C of EKMS 5 (series) contains a list of components contained as part of Repair (Q Kits) to create local inventory documents for verification when conducting page checks, as required.

(1) To conduct a page check of printed COMSEC material, compare each page in the publication against its LOEP.

(2) Each page listed on the LOEP must be in the publication and each page must reflect the correct status. For example, pages identified on the LOEP as "ORIGINAL", must be

ORIGINAL pages. Pages identified on the LOEP as being a specific amendment page (e.g., 1 or AMEND 1), must be that specific amendment page.

g. **Verify Mandatory Modifications**: Verify the installation of DON and NSA mandatory equipment modifications in accordance with Annex W using EKMS 5 (series) and/or the NSA Mandatory Modification Verification Guide (MMVG) as follows:

(1) Should an examination of the equipment indicate a requirement to install a mandatory modification, the EKMS Manager will ensure that the mandatory modification is installed by an appropriately qualified maintenance technician as specified in the instructions accompanying the modification.

(2) Before transferring equipment, the EKMS Manager will also ensure that the modification or MOD Record Plate on COMSEC equipment accurately reflects all installed modifications.

NOTE: See Annex W for additional page checking requirements for other COMSEC material.

h. **Report Page Check or Other Discrepancies**: If a discrepancy is noted during the page check and verification procedures of COMSEC material, the discrepancy must be reported in accordance with Annex V.

758. CONDUCTING PAGE CHECKS AND VERIFYING COMPLETENESS OF COMSEC EQUIPMENT/HOST DEVICES HAVING EMBEDDED CRYPTO OR CCI COMPONENTS:

a. EKMS Managers and LEs/Users shall **not** open host devices/equipment to verify the presence of embedded crypto/CCI components. The presence of these items shall be assumed on the basis of whether or not the host device/equipment is operating as designed.

b. Only CRFs/maintenance depots shall open host devices/equipment containing embedded items and then only as required in support of CRF/maintenance depot inventories or to effect needed repairs (i.e., change out/replace inoperable components).

760. APPLYING STATUS INFORMATION TO COMSEC MATERIAL:

a. Status information (i.e., effective and supersession dates) must be annotated on all COMSEC keying material, COMSEC accountable manuals, and publications upon receipt **except** for large accounts (i.e., 500 or more line items). Large accounts must enter status information on the A/I Summary and annotate the status information upon issue to LEs. Since the status of COMSEC material may be affected by loss, compromise, or operational deviations, EKMS Managers must determine the most current status of material prior to issue, transfer, and destruction.

b. The only authorized source document for the destruction of superseded keying material is the Controlling Authority's COMSEC Effective Status Message or SIPRNET web page. Although status information for keying material (including keying material designated for NATO use) is contained in the SCMR, it is to be used for situational awareness only. Therefore, it is paramount messages promulgated by the material's Controlling Authority and other COMSEC-related General Messages (ALCOM, ALCOMLANT ALFA, ALCOMPAC P) are retained on file and consulted when applying status information, issuing material or performing destruction.

c. The status of COMSEC manuals and publications is normally listed on the Letter of Promulgation (LOP) page within these documents. When not listed, the originator of the document promulgates status via separate correspondence.

d. The generating facility of AL Code 7 material promulgates the effective and supersession dates for ALC 7 material locally generated and must promulgate/disseminate this information to holders of the keying material.

e. **Procedures for Applying Status Information**:

(1) **Canister packaged keying material**: Status will be applied to canister packaged keying material using either a grease pencil, non-permanent ink or marker (i.e., ink markings that can be completely and easily removed for canister inspection), or a zip-lock bag as detailed below:

(a) Grease pencil or non-permanent ink or marker: Only grease pencils or non-permanent ink or marker may be used to apply status directly to the outside of a canister. The use of permanent ink markers/pens for this purpose is **prohibited** as these markers inhibit proper canister inspection.

NOTE: Applying tape or other labels directly to the surface of keying material canisters is strictly

prohibited. This unauthorized practice hides intrusion or penetration efforts and hamper inspection procedures.

(b) Zip lock bag: Apply an adhesive label to the outside of the zip lock bag with the short title of the keymat, edition and the effective and supersession dates annotated on the label. Enclose the associated keying material canister in the zip lock bag.

NOTE: When using the zip lock bag, the adhesive label can be color-coded to help distinguish between 1-month and 2-month key. For example, a white label could be used to identify 1-month key, a yellow label (using a yellow highlighter to ″paint" a white label) to identify 2-month key.

(2) **Other Protectively Packaged Keying Material**:

(a) The status of other protectively packaged keying material sealed in its original packaging must be marked on the plastic wrapper. Do not affix tape or labels to the packaging material.

(b) Upon opening the keying material for use, transfer the status information to the front cover of the material.

NOTE: Status information placed on canisters or other protective packaging must be removed prior to transfer of material to another account.

(3) COMSEC Material in Book or Booklet Form, Manuals, and Publications: Apply applicable status information on the outside front cover so that it does not cover any manufacturer printed data.

(4) Electronic Keying Material: Status information must be maintained, managed and updated in LCMS for electronic key to ensure keying material is issued, used and destroyed when authorized.

f. **NSA Barcode Labels on Keying Material Canisters**: NSA applies barcode labels to the outside of key tape canisters. Although unclassified, NSA barcode labels require special handling at the account level.

Handling instructions for EKMS Manager:

(1) Remove barcode labels from canisters upon initial receipt or prior to issuing or destroying the material and disposing of the canister. Once removed, examine the area beneath the removed label for signs of tampering or penetration.

(2) If tampering or penetration is suspected or evident, retain materials and immediately report as a COMSEC Incident in accordance with Chapter 9. Otherwise proceed with remaining instructions.

(3) Apply the removed labels to a plain piece of paper. NSA requires that the labels be destroyed separately from their associated canisters to prevent the labels from jamming and/or damaging disintegrator equipment. Destroy the pieces of paper (with labels attached) by approved shredder, knife mill, or incinerator.

NOTE: Commands and activities that supersede large quantities of material and use an approved bulk secure destruction process for canister material may destroy canisters without removing labels and without inspecting the area beneath the removed labels.

763. LCMS ACCOUNTABLE ITEMS (A/I) SUMMARY:

a. The Accountable Items Summary (A/I) in LCMS is used to track and manage **all** AL Code 1, 2, 4, 6, and 7 COMSEC material (including modern keys), held by an account. LEs (Using) will use a watch-to-watch inventory to meet this requirement.

b. For accounts equipped with a LMD, the A/I Summary will be maintained and generated from LCMS.

c. EKMS Managers and Local Elements (Issuing) will maintain an up-to-date print out of the A/I Summary. It is recommended that accounts print out the AIS from LCMS when the Transaction Status Log is printed as outlined in Annex T to minimize the impact should an account experience a failure of the LMD and not have a current LCMS database backup to restore from in reconstructing the AIS.

NOTE: At the discretion of the command, at the account level, the monthly COAL inventory can be printed and maintained in lieu of the entire AIS.

d. EKMS Managers will provide LCMS-generated A/I

Summaries to LEs (Issuing) and instruct them on their maintenance, **or** the LEs (Issuing) may generate the A/I summaries locally. In either case, the responsibilities for generating and maintaining them shall be clearly understood and agreed upon by both parties.

e. The A/I Summary must be retained per Annex T.

766. **EKMS INVENTORIES**:

An LCMS operator is required to periodically perform an inventory to verify the existence of material accountable to the account or LE. LCMS enables the operator to create, process, and reconcile inventory reports. The following inventory scenarios are supported by LCMS:

-- Inventory is initiated by the account for its own use in verifying its material holdings.

-- Inventory is initiated by the account in response to a specific request from the COR.

-- A COR account generates an inventory report for an account.

Twice each calendar year, on a fixed cycle, Tier 2 accounts will receive a "Request for Inventory Transaction/Type 18)" from the COR. An explanation of this process can be found in Article 766.f.

NOTES: (1) To negate the need for individual waivers, submarines on deployment or patrol which are unable to establish connectivity via the X.400 to download required inventories to satisfy requirements contained herein will conduct the inventory on the same interval or occasion, as applicable, using a locally generated inventory from LCMS. At the earliest possible opportunity, an inventory completion message must be submitted as discussed in 766.f.4.

AMD-9

With exception to inventories used solely for documenting a Change of Command, EKMS Managers must report completion of all account inventories to NCMS via official naval message.

(2): All inventory related documents, i.e. individual working documents generated for the account and LE level,

AMD-9

consolidated (complete) reports, related accounting reports for any alternations to the physical inventory and inventory completion messages or online reporting forms must be signed and retained on file in accordance with Annex T. Missing or unsigned reports will be handled in accordance with Articles~~ 945.e.16 or ~~1005.a.

a. **Inventory Requirements**:

(1) Semi-annually: All COMSEC material (including equipment and publications) assigned AL Code 1, 2, 4, 6, and 7 must be inventoried semi-annually (twice each calendar year (CY)).

(2) Inventory Results to be Reported: In accordance with Article 766.b.1, the results of semi-annual inventories of AL Code 1, 2, and 6, Change of EKMS Manager (CCIR) inventories, and combined inventories must be reported to the COR when required to be conducted. Inventory results for AL Code 4 and 7 keying material will be retained at the command in accordance with Annex T.

(3) **Change of Command (COC) or Staff CMS Responsibility Officer**: Prior to the relief or detachment of the Commanding Officer, **all** COMSEC material will be inventoried, unless a Staff CMS Responsibility Officer (SCMSRO) has been designated. If so, the relief or detachment of the SCMSRO is the controlling factor, and an inventory of **all** COMSEC material is required prior to the relief or detachment of this individual. ALC-6 and ALC-7 material will be inventoried through verification of the Accountable Item Summary (AIS) in LCMS.

(a) Signature requirements: The outgoing CO/OIC or SCMSRO, as applicable, will sign the inventory. The incoming CO/OIC or SCMSRO (as applicable) may initial, if desired, but it is **not required.**

(b) Preprinted signature identification entries must be adjusted as necessary (e.g., SCMSRO vice CO/OIC).

(c) The inventory will be retained at the command in accordance with Annex T.

(d) An inventory will be requested from the supporting account and conducted by the external LE (LE Issuing or LE Using) without their own six-digit account supported through a Letter of Agreement within 30 days of a Change of

Command.

(4) **Change of EKMS Manager**: The COR must be notified via official naval message or digitally-signed PKI email to ncms_nafw_cor@navy.mil no later than 10 days prior to the start date of a Change of EKMS Manager inventory. Once notified, NCMS will initiate the inventory process by sending a Request for Inventory Transaction. All COMSEC material will be inventoried and the results will be reported to the COR via the Message Server; the hard copy (signed) inventory will be retained at the command in accordance with Annex T. A CCIR or combined inventory used to conduct a Change of EKMS Manager must be reconciled by the COR, preferably prior to detachment of the outgoing EKMS Manager. The outgoing EKMS Manager will remain responsible for material charged to the account up to their detachment date, pending COR reconciliation. Per Article 455 and Annex Y to this manual, the EKMS Manager Turnover Checklist must be completed when an account turnover occurs.

AMD-9

Annex AJ provides a description of common errors managers may encounter, as well as a description of causes and recommended resolution actions.

NOTE: When a new LE Issuing is appointed, an inventory is required and will be conducted by the outgoing LE Issuing and witnessed by the incoming LE Issuing. Such inventories will be requested from the parent account EKMS Manager. The original completed and signed inventory will remain on file with the LE Issuing with a copy submitted to the supporting accounts EKMS Manager.

b. **Types of EKMS Inventories**: There are five types of EKMS inventories: Semi-Annual Inventory Report (SAIR), Change of Custodian or Change of Command Inventory Report (CCIR), a Combined Inventory, a Change of Account Location (COAL) inventory and a Consolidated Inventory.

(1) **Semi-Annual Inventory Report (SAIR)(also referred to as a Fixed-Cycle (FC) Inventory)**:

(a) Inventories will be conducted, at a minimum of semi-annually and will include; all keying material, equipment and publications as well as required page checks.

(b) Twice each CY, at six-month intervals determined by the EKMS account number (see Fixed-Cycle Inventory Schedule), the COR will electronically transmit a ***Request for Inventory***

Transaction to each account. Once opened, this request will prompt the account to submit a SAIR. No later than 30 days after receipt of the initial Request for Inventory Transaction, the account must generate an inventory with the COR as the destination EKMS ID and submit the inventory via the message server to the COR. Procedures for electronically submitting a SAIR can be found in EKMS-704(series).

(c) The process above is not related to the physical conduct of an inventory but is used to identify accounting discrepancies between the COR and the units Accountable Item Summary (AIS). Accounts have up to 90 days to generate and submit an electronic inventory to the COR, complete the physical inventory (including applicable page checks), report completion by message and self-reconcile the inventory.

(d) After electronic submission of the SAIR to the COR, the COR will respond with an electronic Inventory Reconciliation Status Transaction (IRST) (Type 17). The IRST identifies the discrepancies between the Tier 1 database and the local Tier 2 database.

(e) If discrepancies are identified in the IRST, it is the responsibility of the EKMS Manager to work diligently with the COR to resolve any discrepancies in a timely manner. Guidance to assist the manager in the understanding and resolution of inventory discrepancies can be found in Annex AJ. If not resolved and manual intervention is necessary, the COR will correspond with the account to correct the discrepancies. The COR Manager will assist the account in clearing all discrepancies that appear on the IRST. It is the responsibility of the EKMS Account Manager to actively pursue resolution of all IRST discrepancies in order to achieve a final reconciliation of the inventory. The IRST must be reconciled with the COR and all discrepancies resolved or documented to the COR Account Manager within 90 days from the date of the original request for inventory transaction. AMD-9 **Failure to self-reconcile the account's inventory within 90 days will result in a PDS and the command being included in ALCOM message identifying delinquent accounts.**

(f) The COR will monitor the response to inventory transactions and will notify commands that fail to return a reconciled inventory within 30 days. The COR will initiate tracer actions as follows:

First tracer notification will be sent 30 days after the event date as an EKMS transaction to the delinquent command by Tier 1.

Second tracer notification will be sent 60 days after the event date as an EKMS transaction to the delinquent command by Tier 1.

Third and final tracer notification will be sent 90 days after the event date as an EKMS transaction to the delinquent command by Tier 1.

DELAYS IN THE SUBMISSION OF SAIR INVENTORIES MUST BE REPORTED TO THE COR PRIOR TO THE REQUIRED DUE DATE

1. **FOR SSBN/SSGN ONLY**:

a. The Crew turnover inventory may be submitted to the COR for reconciliation.

b. The first Crew Turnover SAIR must be submitted at the beginning of the calendar year for reconciliation, and shall report inventory results of all COMSEC material, including manuals/publications and equipment holdings.

c. Crew Turnover SAIR shall be submitted NLT 30 days after the turnover.

d. Annotate the Crew Turnover inventories as follows: “THIS INVENTORY SUBMITTED FOR FIXED-CYCLE INVENTORY”.

e. The third change of command inventory of the year will be conducted in its entirety to include all COMSEC material, including manuals/publications and equipment holdings, and sent to the COR.

2. **HULL AND CREW SWAPS**:

a. Crew swaps are conducted within a single EKMS account. In addition to the requirements set forth in this article, units which perform crew swaps within a single account will follow the inventory procedures established in article 766.b.1.g.1 above.

b. Hull swaps involve personnel from one ship transferring to another ship and vice versa.

c. For hull swaps, a consolidated change of command and change of custodian inventory requested from the COR is required on both ships. The inventory will be conducted by the manager from ship "a," witnessed by the manager from ship "b" and signed by the CO of ship "a." This process will be reversed for the other ship as each has its own six-digit COMSEC/EKMS account.

d. Central Office of Record (COR) notification. Surface units conducting either crew or hull swaps must notify the COR via naval message no later than 120 days prior to the turnover. To ensure proper chain of command visibility, units will include their ISIC on these messages.

e. With exception to operational SSBNs and SSGNs not undergoing a maintenance availability, fixed cycle inventory dates and the requirement for conducting semi-annual inventories do not change as the result of crew or hull swaps. The account's most recent reconciliation must be within 6 months of a crew or hull swap, as applicable. If the most recent reconciliation is more than 6 months old, the account's EKMS Manager must ensure the latest Change of Account Location (COAL) inventory reflects zero discrepancies NLT 30 days prior to the crew or hull swap, as applicable.

> **Note: SSBNs and SSGNs when operational are exempt from fixed-cycle inventory requirements. This latitude is community specific because the frequency of inventories conducted for crew swaps which are submitted to the COR for reconciliation is greater than the inventory requirements set forth at both the National and Navy level. During extended maintenance availability Periods, SSBNs and SSGNs will adhere to their normal fixed cycle inventory cycle to ensure compliance with National and Navy policy.**

f. Units involved in either a crew or hull swap must request a consolidated inventory (change of command combined with a change of custodian) via naval message no later than 30 days prior to the crew swap. The message must include the date of the latest inventory. If the swap occurs in the same calendar month as the account's fixed cycle inventory period, a single combined inventory may be used to satisfy the fixed cycle, change of command, and change of custodian inventory requirements in lieu of conducting separate inventories for each.

g. Inventory reporting: Upon completion of the physical inventory, notify NCMS and the ISIC of the

AMD-9

completion by naval message in accordance with Article 766 (note) above. ~~Use of the inventory completion form on the NCMS NIPRNET Portal is not authorized for crew and hull swaps.~~

h. Proper planning is essential for units involved in hull swaps, particularly when a ship is changing homeports and is not already validated for keying material that is theater specific.

i. It is imperative when either a hull swap or crew swap is conducted the off-going personnel log on to the LMD and allow the on-coming personnel to change both passwords and pins associated with the LMD. Ensure the root Password is provided to the on-coming personnel, changed and recorded on a SF-700. The oncoming personnel assuming responsibility for management of the account will, at the time of the change, properly prepare new SF-700s in accordance with Articles 515 and 520. Additionally, combinations to locking mechanisms for restricted areas, security containers and vaults must also be changed and the associated SF-700s updated.

j. When a hull or crew swap is conducted, both CMS Form-1s and USTC Form 10s must be updated to ensure account personnel are on file for their respective (not prior account for hull swaps) account or they will not be able to pickup material from CMIO or DCS, as applicable.

k. Both Common Account Data (CAD) and Central Facility User Representative Forms (CF 1206 forms) must be updated. Updating of CAD data has no relation to ordering privileges for modern key.

l. When a hull swap or crew change is conducted the oncoming EKMS Manager for the account will perform both a KP changeover and KP rekey.

(g) The following table illustrates when each account can expect a SAIR (FC). With exception to SSBNs, SSGNs and SSNs, NCMS will not approve requests to change inventory cycle dates reflected below.

FIXED-CYCLE (FC) INVENTORY SCHEDULE

If your EKMS ID number is:	1st FC SAIR for CY:	2nd FC SAIR for CY:
100000 through 158500	January	July
158501 through 199999	February	August
200000 through 258100	March	September
258101 through 299999	April	October
300000 through 358200	May	November
358201 through 399999	June	December

EXAMPLE: If your EKMS ID number is 123456, your account will be prompted to generate its first FC SAIR in January of each CY. The FC SAIR must be completed in its entirety (i.e., key, equipment, and publications/manuals (including page checks for publications and Q-kits) must be inventoried) and sent via the message server to the COR for reconciliation. In July of each CY, your account will again be prompted to send a second FC SAIR of the CY. All COMSEC material must be inventoried in its entirety (i.e., key, equipment, and publications/manuals must be inventoried) and sent via the message server.

(h) If a Request Inventory transaction is received for an inventory which is not in line with the above reflected schedule, contact the COR so the schedule discrepancy can be corrected.

(i) EKMS Managers have 30 days from receipt of the Request Inventory Transaction prompt to send the FC SAIR to the COR. Do **not** wait until the inventory is physically completed before sending the electronic inventory to the COR. Non-receipt of the Request Inventory Transaction does not relieve the EKMS Manager from compliance with the minimum inventory requirements of this article.

(j) Step-by-step inventory guidance is reflected in Article 766.f.

AMD-9

(k) Failure to complete, return, and maintain signed inventories on file in accordance with Annex T and self-reconcile the accounts inventory must be reported in accordance with Article ~~945.e~~1005.a unless an extension is approved by NCMS in writing.

(3) **Change of Custodian Inventory Report (CCIR)**:

(a) The purpose of the CCIR is to satisfy National and Navy policy which require that an inventory be completely conducted, documented, reported to and reconciled by the COR for documenting a Change of EKMS Manager.

(b) A CCIR is also used to document a change of command.

(c) CCIRs used **solely** to document a change of command, will be retained at the command and completion reporting to the COR is not required. If the inventory requirement for a change of command and a semi-annual inventory are combined, completion must be reported to the COR via message.

(d) Results of inventories used to document change of an alternate EKMS manager or change of a LE Issuing do not require reporting to the COR but the signed inventories will be retained at the command in accordance with Annex T.

(4) **COMBINED INVENTORY**:

(a) A SAIR and CCIR is occasionally used to satisfy the requirements of both a Semi-Annual Inventory Report (SAIR) in conjunction with change of command or change of EKMS Manager, as applicable.

(b) A SAIR may be COMBINED with a CCIR when, and only when, the occasion for the CCIR occurs within the same or following calendar month as the SAIR and only after receipt of the SAIR Request for Inventory Transaction (RIT) date (on or after the 7th of the month). The physical inventory must be completed and signed within 60 days from the date of the RIT. The EKMS Manager has an additional 30 days (total 90) to resolve any accounting related discrepancies with the COR.

(5) **CHANGE OF ACCOUNT LOCATION (COAL) INVENTORY**:

(a) A primary management tool intended to assist EKMS Managers in determining the health and status of the account. **Except as indicated in (c)~~(b)~~ below**, at a minimum of monthly, EKMS Managers will generate a COAL inventory and

AMD-9

wrap/submit the inventory to Tier 1 to obtain an Inventory Reconciliation Status Transaction (IRST) in accordance with the procedures outlined in the EKMS-704 (series).

(b) Upon receipt of the COAL, the COR will transmit an Inventory Reconciliation Status Transaction (IRST) to the EKMS Manager. The EKMS Manager will then initiate the reconciliation process discussed in Article 768 and Annex AJ.

(c) Submarines at-sea are exempt from the monthly requirement noted above when deployed but will generate a COAL within 30 days prior to departure and upon return from at-sea period.

NOTE: Unlike SAIR, Change of Command, Change of EKMS Manager or Consolidated Inventories, a COAL inventory does not have to be printed and physically completed. Although a physical inventory is not required, all IRST discrepancies must be researched and resolved within 5 working days.

(6) **CONSOLIDATED INVENTORY**. Is intended to be used to document a simultaneous Change of Command and Change of EKMS Manager.

AMD-9

(a) A consolidated inventory **must be requested by the account and initiated by the COR** as discussed in 766.a.4 above.

(b) The inventory will be conducted by the outgoing Manager and witnessed by the incoming Manager.

(c) CO signature requirements will be in accordance with Article 766.a.3.a above.

(d) An inventory completion message is required in accordance with Art 766 note.

(e) This may also be used in conjunction with a SAIR but when so done must be completed within the same timeframe as a combined inventory (discussed above).

c. **Miscellaneous EKMS Inventory Policy**:

(1) Extended Absence of EKMS Manager. If the EKMS Manager is or will be absent for more than 60 days, a new EKMS Manager **must** be appointed and a Change of Manager Inventory

conducted.

(2) Waiver of Inventory Requirements in a COMBAT Environment:

(a) When operations in a combat environment preclude completion of a required EKMS inventory, the requirement will be waived until operational circumstances permit inventory completion. It is the responsibility of the EKMS Account Manager or the ISIC to advise NCMS of the estimated duration of the combat environment deployment. A complete inventory cycle must be conducted no later than 45 days following completion of the combat situation.

(b) Affected commands or ISICs must notify NCMS//N3// by message as soon as practicable that submission of the required inventories will be delayed. When circumstances permit resumption of normal account activities, both CORs must again be notified by message.

(3) Inventory of Material in Spaces to which the EKMS Manager is **NOT** normally Authorized Access:

(a) If operational considerations preclude allowing either the EKMS Manager or Alternate access to a space, the individual responsible for the COMSEC material in the spaces must provide the EKMS Manager with a properly completed local inventory, must certify in writing that all required page checks were conducted, and inform the EKMS Manager of any page check discrepancies.

(4) Inventory of Material Issued on Local Custody:

NOTE: Use "Originate Inventory Report" procedures in Chapter 4 of the LMD/KP Operators Manual with a destination of "local element" selected.

(a) An EKMS Manager may direct LEs to inventory the COMSEC materials for which they have local custody responsibility. The account EKMS Manager is encouraged, however, to conduct the sight inventory of material held on local custody when possible, particularly on the occasion of either a Change of Custodian or Combined inventory.

(b) Results of a LE inventory must be reported in writing to the EKMS Manager. The inventory may be recorded and reported on a SF-153 or another form previously approved by the

EKMS Manager. Upon receipt of these signed LE inventories, the EKMS Manager must reconcile the generated account inventory within LCMS.

(c) Local inventories will be retained at the command in accordance with Annex T, and will not be forwarded to the COR or NCMS.

(5) Material Temporarily held by a CRYPTO Repair Facility (CRF) or Maintenance Pool:

(a) Material temporarily (i.e., less than a year) in the custody of a CRF or a maintenance pool may be inventoried by sighting the local custody document for the material.

(b) If the material has been in the custody of the CRF or maintenance pool for more than 1 year, the CRF or maintenance pool must verify, in writing to the Manager, that the equipment is in their custody, or the Manager must personally sight the equipment.

d. **Documenting an EKMS Inventory**:

(1) All inventories must be documented on a SF-153, reflect all required signatures as stated in Annex U paragraph 7.a, and be retained in accordance with Annex T.

(2) AL 4 material may be inventoried either by; (1) generating an inventory at the parent account LMD and making the local account the destination for the inventory, (2) creating a local SF-153 outside LCMS and transcribing the information from the working copies of inventories generated for the local account and each LE in which material is issued to, or (3) by having all working copies originated signed by the two personnel actually inventorying the material and the CO. ALC-7 material will be inventoried through verification of the Accountable Item Summary (AIS) in LCMS. Effective with AMD-8 ALC-7 material does not have to be manually transposed on a SF-153 outside LCMS. Options (1) or (2) are the preferred and recommended methods to negate the need for a CO to have to sign numerous working copies.

NOTE: A print out of the AIS will not be used for this purpose. EKMS-704 provides guidance in how to generate an inventory from the LMD. Although any method described above may be used procedurally to inventory AL 4 and 7 material, it must be understood the material must be

inventoried and such must be verifiable.

(3) To document Found, Lost or Missing Material:

(a) Submit either a COMSEC Incident Report or a reportable PDS in accordance with Article 945 or 1015, as applicable. Article 1015 would only apply if the material is unclassified, not marked or designed as crypto and not CCI.

(b) A Relief from Accountability report will not be generated by the account until so authorized by the COR following evaluation and assessment of the related Incident or PDS, as applicable.

(c) Material found outside of required accountability (not on the local AIS) will not be possessed without prior approval of the Service Authority. See Article 739.d, 739.3 and the note which follows.

e. **Conducting the Inventory**:

(1) Who May Inventory COMSEC Material:

(a) A CCIR Inventory conducted due to a Change of Manager **must** be conducted by the outgoing Manager and witnessed by the incoming Manager.

(b) If the outgoing Manager is physically incapacitated, the inventory must be conducted by the Primary Alternate Manager of the account and incoming Manager.

(c) All other inventories must be conducted by the account EKMS Manager or Alternate and a qualified EKMS witness.

(d) LE Inventories must be conducted by the person having local custody responsible for the material and a qualified EKMS witness.

(2) How to Inventory COMSEC Material:

(a) All individuals conducting an inventory must sight the short title, edition suffix, and if applicable accounting (serial/register) number of each item of AL Code 1, 2, or 4 COMSEC material held by the command. The individual conducting an inventory of electronic key stored in the LMD/KP will visually verify all AL Code 6 and 7 material on the Accountable Item Summary (AIS) in LCMS. A witness is not required for inventory of electronic key except for Change of EKMS Manager inventories which will be conducted by outgoing manager and witnessed by the incoming manager.

(b) Unsealed COMSEC materials and the classified components of issued repair or Q-kits must be page checked during an inventory.

(c) Annex W details page check requirements.

(d) EKMS Managers or the TPA, if appointed separately will inspect tamper seals on STEs in accordance with Annex AD paragraph 4.g note 2.

f. **SAIR Tier 1 Inventory Process**: A brief overview of the SAIR process is described below:

(1) Twice each calendar year, the COR sends a ***Request Inventory Transaction*** to a Tier 2 account in accordance with the schedule reflected in Article 766.b.

(2) The Tier 2 account receives and processes the transaction, creating a SAIR with the COR identified as the destination account.

(3) The Tier 2 account wraps the generated inventory and sends it to the COR via X.400 Message Server. Tier 2 accounts must send the generated inventory to the COR as soon as possible and within 30 days of receipt of the Request Inventory Transaction date and must not wait until completion of the physical inventory before doing so.

(4) The Tier 2 account will print and conduct the inventory. The EKMS Manager and witness must properly line-out and initial any alternations and annotate the corresponding transaction number associated with the adjustment. Material transferred or destroyed pending completion and signing of the inventory will be lined as stated above. Upon completion, the account will retain the original hard copy inventory locally. A copy should be forwarded to the COR only if requested by the COR Account Manager. Regardless of the Central Office of Record (COR) servicing the account, all DON EKMS Accounts will submit inventory completion messages to NCMS who also serves as the DON Service Authority for COMSEC matters. Inventory completion messages or inventory completion forms submitted online will be **printed and** retained with the signed copy of the inventory in accordance with Annex T. Failure to submit and retain inventory

completion messages **after** 01 Feb 2011 will be documented in accordance with Article 1005.A.

(5) The COR will respond with an Inventory Reconciliation Status Transaction (IRST) which reflects the differences between the COR and the Tier 2 account's databases.

(6) The Tier 2 account must submit the appropriate accounting transactions to the COR, electronically, when possible, to clear the IRST including **any consolidated destruction reports pending the CO's signature provided such reports have been signed by two account managers or an account manager and a properly cleared second person when another official is not acting in his/her capacity. The CO signature remains required and destruction reports must be signed at the earliest possible date, if the CO is on leave, travel, etc... and unavailable for signature.** There is no need to line out or to make adjustments to the IRST or to return the IRST to the COR. Items that appear as "Short" indicates that something in the records reflects something not held by or reflected in the Tier 2 accounts AIS. The Tier 2 account must provide documentation (transfer, destruction, relief from accountability report) to accurately reflect the disposition of the material. Items that appear as "Excess" indicates that the Tier 2 has something in inventory that is not reflected in the COR database. The Tier 2 account will respond by sending the appropriate accounting transactions (e.g., receipts, possession reports, generation reports (if ALC 6 material is produced, when authorized) to the COR. See Article 768 and Annex AJ for information on account reconciliation actions and discrepancy resolution.

(7) Notice of Reconciliation will not be provided without notification that the inventory has been completed. See Article 766.f.4.

(8) Upon completion of the inventory and once the IRST has been reconciled, the COR will provide a Records Clearance Certificate (RCC) indicating the SAIR is complete.

g. **IRST Accuracy**:

(1) When the destination account of the inventory is either the Local Account or any account other than the COR, only material which is not issued to a LE and is held in the account will appear on that inventory resulting in an inaccurate IRST

being created by the COR.

(2) For all Semi-Annual (SAIR), combined, Change of EKMS Manager (CCIR), and monthly Change of Account Location (COAL) inventories, the COR must be the destination account. This will ensure that all material held in the account, including that issued to a LE, is reflected and will enhance the accuracy of the IRST. Change of Command (unless conducted as part of a combined inventory) and COAL inventories (other than the required monthly report) will use the local account vice the COR as the destination.

767. **INVENTORY BEST PRACTICES/LESSONS LEARNED**:

In an effort to expedite the processing of Accounting Reports and timely completion of submitted Semi-Annual Inventory Reports/Fixed Cycle Inventories (SAIR/FC), the following lessons learned and best practices are provided:

a. All reportable transactions should be submitted to the COR via the appropriate communication methods in a timely manner. If access to the X.400 message server is not available, with prior approval from a COR Manager the use of fax or digitally signed email may be authorized. If authorized, the EKMS Manager is responsible for ensuring that any documents faxed, scanned or emailed are sent via approved media based on any classification markings on the documents.

b. Ensure all Reportable Accounting Transactions are wrapped and sent to the COR for the account (616502 FOR PT1S SAN ANTONIO; 5A8240 FOR PT1S FT HUACHUCA) with a copy sent to the originating account as well.

c. Transactions should be submitted in the order in which they occur and NLT than 96 hours of action (Receipt/Transfer). To minimize accounting history errors and/or inventory discrepancies, do not submit transactions out of order or all at once in bulk.

d. Only submit COR reportable transactions once (unless otherwise requested by a COR Account Manager). Local transactions (examples: local custody issue documents, local destruction reports, local generation reports, local inventories, etc...) and multiple submissions will result in rejection by the COR.

e. Material must be receipted for or possessed, as applicable with such reported to the COR and reflected on the account’s AIS prior to the transfer of the material or submission of a Destruction Report for the material. Failure to do so will cause accounting and inventory discrepancies in the COR’s database upon receipt of a subsequent transfer or destruction report. Unless otherwise stated, the below accounting functions must be reported to the COR and when adhered to will aid EKMS Managers in effective account management:

(1) Reportable Destruction for all material (ALC 1, 2, 6) must be reported to the Tier 1 COR.

(2) Transfer Report Initiating (for material transferred to another COMSEC Account).

(3) Transfer Report Receipt Individual (when reconciling for material using a Hard Copy report. Authorized only when an electronic receipt is not available to reconcile the material with).

(4) Transfer Report Receipt All (when reconciling for material using an electronic report).

(5) Reportable Generation Report (when ALC 6 key is generated, if authorized).

(6) Possession Reports. Except when created; as a result of a system rebuild, to correct a typographical error.

(7) Relief From Accountability (RFA). Except when created; as a result of a system rebuild, to correct a typographical error.

(8) IRSTs must be processed and reconciled at a minimum of monthly to ensure the account is well maintained and prevent problems when inventories are required.

Note: Some CCI equipment, i.e. KG-175s for example may have a letter either before or after the serial number of the device. The COR tracks the numerical serial number without regard to whether the letter is prior to or after the serial number.

768. IRST RECONCILIATION RESPONSIBILITIES:

An inventory reconciliation status transaction (IRST) is generated automatically by the COR upon submission of an EKMS inventory. The following subparagraphs outline the responsibilities associated with account reconciliation and provide guidance and procedures for reconciling received IRSTs. Each IRST received by the EKMS account from the Central Office of Record (COR) must be reviewed and processed by the EKMS Account's Management team (Primary and Alternate EKMS Managers).

a. **EKMS Account Reconciliation Responsibilities**:

(1) Upon submission of a SAIR, CCIR, Combined or Consolidated inventory, the EKMS Management team is responsible for reviewing the received IRST and initiating the process of reconciling the listed discrepancies in accordance with Annex AJ. The majority of discrepancies reflected on the accounts IRST can be reconciled by the primary or alternate EKMS Managers without assistance from a COR Manager. **Therefore, it is essential that the first course of action for the EKMS Manager to take to reconcile IRST discrepancies is following the instructions listed in Annex AJ.**

(2) Should the primary or alternate EKMS Manager require assistance in reconciling discrepancies and **a COR Manager has not been assigned**, the account should submit a digitally signed email to: ncms_nafw_cor@navy(.smil).mil. A team of COR Managers are consistently monitoring these email accounts and will respond to inquiries as quickly as possible and no later than 3 working days. To avoid unnecessary delays in receiving assistance, do not contact COR Managers directly for assistance. Assistance from NCMS will be provided through the use of the ncms_nafw_cor@navy(.smil).mil email address. Include the account number in the subject line.

(3) Regardless of previous contact with other NCMS personnel in reconciling the account, the EKMS Manager must always coordinate and remain in communication through resolution with the COR Manager assigned to the account. Failure to inform the assigned COR Manager of the accounts reconciliation efforts including providing the Date Time Group for any COMSEC incident messages or bad Bulk Encrypted Transaction (BET) reports **will** impede and unduly delay reconciling the account.

(4) Deadlines for account reconciliation are reflected in Article 768.d below.

b. **COR Manager Reconciliation Responsibilities:**

(1) NCMS COR Manager is responsible for assisting the EKMS Manager during the reconciliation process. **EKMS Managers are ultimately responsible for the COMSEC account's reconciliation.**

(2) EKMS Managers must be engaged, proactive and make every effort to maintain communications with the COR Manager until the account is fully reconciled.

(3) COR Managers will make every effort possible to ensure the EKMS account is fully reconciled within the established timeframes. However, the COR Manager's involvement is contingent upon ongoing cooperation, engagement and the supplying of applicable accounting reports by the EKMS Managers. Failure of an EKMS Manager to complete the necessary actions, as directed by the COR Manager will delay or prevent the reconciliation of the account.

c. **Change of Account Location (COAL):**

(1) The purpose of the COAL is to provide EKMS Managers with a monthly assessment of their EKMS account. Once the COAL has been submitted and the IRST is received, the EKMS Manager shall execute the reconciliation process discussed in Article 768.a.1 above. Reconciling of the received IRTS's monthly greatly enhances the management of the account as well as improves the accounts ability to reconcile inventories within the required timeframes.

(2) Assistance with reconciling IRST discrepancies which result from the submission of the COAL will be through submission of related inquiries to the currently assigned COR manager or, if not assigned, to: ncms_nafw_cor@navy.mil.

(3) Failure to submit and reconcile monthly COALs will result in significant delays in completing the inventory reconciliation process.

d. **Reconciliation Deadlines:**

(1) The deadline for completing the IRST reconciliation process is 90 days.

AMD-9

(2) Failure to achieve 100% reconciliation within 90 days will result in a PDS and account being included in a monthly ALCOM identifying all delinquent accounts.

(3) When necessitated due to operational commitment, ongoing unresolved discrepancies, etc. NCMS may grant an extension to ensure the account is properly reconciled. Extensions will be dependent on the active involvement and engagement by the accounts EKMS Manager or Alternates. Waivers must be requested via naval message and must include the units ISIC and TYCOM as info addees.

769. **ISSUING COMSEC MATERIAL**:

a. **Responsibility**:

(1) Managers are responsible for the proper movement, both internally and externally, of all COMSEC material held by the account.

(2) Movement of all COMSEC material must be coordinated with the EKMS Manager.

(3) COMSEC material will be issued for use only after determining that the intended recipient is properly cleared, authorized access to keying material in writing and the EKMS Manager has a properly completed SD 572 Form on file for the individual (LE).

(4) All personnel receiving COMSEC material must be provided written instructions for properly accounting for, disposing of, handling and safeguarding for COMSEC material.

(5) To ensure a continuous chain of accountability is consistently in effect, the issuance of COMSEC material must **ALWAYS** be documented on Local Custody documents which will be maintained by the EKMS Manager or LE Issuing and the LE Using in accordance with Annex T.

b. **Local Custody Defined**:

(1) Local custody is the acceptance of responsibility for the proper handling, safeguarding, accounting, and disposition of COMSEC material issued by EKMS Manager and LE personnel.

(2) Every person to whom COMSEC material is issued or with access to classified COMSEC material must complete a SD Form 572 in accordance with Annex K.

NOTE: 1. Authorized users of the Tactical Aircraft

Mission Planning System (TAMPS) not directly issued GPS key need not complete a SD 572 Form, but must hold a SECRET clearance.

2. Electronic signatures are acceptable on SD Form 572s, provided all legal requirements (e.g., authenticity, non-repudiation, verification, and records management/storage) are met. Legal requirements include, but are not limited to, Article 15 U.S.C. 7001, 7006 and 7021. DOD CAC or NSS PKI Tokens meet these requirements.

c. **Local Custody Issue (LCI) Forms**:

(1) A SF-153 or a locally prepared equivalent form may be used to properly document the local custody issue of COMSEC material. The minimum information required on locally prepared forms is as follows:

(a) Issued by.
(b) Issued to.
(c) Short title, quantity, accounting (serial/register) number and AL Code(s) of material issued.
(d) Date.
(e) Signature(s).

Signature Requirements: Local Custody documents reflecting TS material will **always** require two signatures. Unless otherwise stated by local, ISIC, or TYCOM policy only one signature is required for Local Custody documents reflecting only Secret and below material or unkeyed CCI equipment.

NOTE: If key is loaded/filled in an electronic storage device including but not limited to; KYK-13, KYX-15, DTD, SKL or TKL and any of the key stored/issued is TS, two signatures are required.

EKMS Managers and Alternates will not sign local custody documents either as "received by" or as a witness for COMSEC material issued to LEs unless the Manager/Alternate is also assigned to/in charge of the respective LE. Material not held at the account level (vault) will be signed for and witnessed (if required) by LE personnel assigned to the respective work center where the material is used and/or stored.

(2) The issuing Manager must retain the original copy of the signed and dated local custody document and provide a copy to the individual receipting for the material for the LE's local custody files. A signed local custody form indicates assumption of responsibility for the material listed thereon.

d. **Local Custody File**:
Both EKMS Managers and Local Elements (LEs) must maintain a local custody file containing effective, signed local custody documents for all material issued. Local custody files will be maintained as outlined in Annex T.

e. **Time Periods for Issuing COMSEC Material**:

(1) Equipment, publications, and other material not marked or designated CRYPTO may be issued at any time prior to the effective date of the material.

(2) COMSEC keying material in either hard copy or electronic form which is marked or designated CRYPTO, may **not** be issued any earlier than 30 days prior to the effective period (month) of the material except as indicated in Annex Z paragraphs 13.c.1 and 13.c.2.

(3) Refer to Article 769.f for GPS key issued for use with Tactical Aircraft Mission Planning System (TAMPS).

NOTE: Authorization to issue keying material marked or designated "crypto" more than 30 days prior to the materials effective date, except as indicated above requires a waiver from the Controlling Authority.

The restriction above does not apply to black key which is considered UNCLAS/FOUO when encrypted using an approved means such as the LMD/KP or the CWMS/DMD PS. When concurred with by the Controlling Authority both current and future editions may be issued in a black key package without authorization from NCMS provided the KEK is withheld by the LE Issuing or EKMS Manager until a reasonable time before the effective period of the keying material with which it is associated. Sound risk management should restrict the number of editions included in a black key package to that which is operationally required.

(4) LEs may be issued one edition of WHENDI (when directed) material.

f. **Issue of COMSEC Keying Material In Hard Copy Form To Mobile Users or Navy Expeditionary Combatant Commands (NECC)** :

Mobile users or Navy Expeditionary Combatant Commands (NECC) (i.e., Marine Tactical units, Naval Special Warfare (SPECWAR) units, Naval Construction Battalion units, and Explosive Ordnance Disposal (EOD) units, and all aircraft) are authorized issue of a sufficient quantity of keying material to support mission requirements.

NOTE: Mobile users in this instance do not include U.S. ships, with the exception of Littoral Combat Ships (LCS).

Issue keying material as follows:

(1) Paper Copy Form Under **Normal** (Peacetime) Conditions:

(a) When possible to preserve the integrity of the protective packaging, issue paper copy key as whole editions.

(b) When necessary to issue extracts or individual segments of keying material, no more than three segments (effective plus two) of any short title will be issued. The segments will not be removed from the protective packaging until immediately before issue.

(c) If more than three segments of a short title are required to complete a mission, the entire edition will be issued.

(d) During issue, issuing elements and recipients (e.g., LEs) will verify and acknowledge receipt of the segments and then jointly reseal the non-effective segment(s) as outlined in Article 772.

(e) Airborne units that are issued the entire edition and require frequent access to the final copy of a multi-copy keytape segment during rotating flight operations, are authorized to place the final keytape segment in a zip lock bag with the original canister of material (i.e., the loose segment need not be sealed in an envelope). Mission essential material will be issued as close to the start of the mission as possible.

(2) Paper Copy Form Issue Under **Combat** Conditions:

(a) Key must be issued in electronic form whenever possible, either in the equipment or in a FD.

(b) When not issued in electronic form, the issuance of an entire canister (edition) of key to front-line positions must be avoided.

NOTE: See Annex Z for the maximum amount of keying material that will be issued in a DTD under real world crisis, contingency scenarios or combat conditions.

(c) A maximum of seven segments of keying material (effective plus six) may be issued to individuals who must be separated from their command or the EKMS issuing point for more than one crypto period when key is not issued in electronic form.

g. **Issue of Keying Material in Electronic Form to LEs**:

(1) If keying material is issued to a LE via a FD, the loading of the FD and issue can only occur just before the planned mission. If the DTD is used, loading of encrypted key may occur 24 hours prior to the planned mission.

(2) Issue of key for Have Quick Radio via FD or hardcopy: Operational requirements and logistical constraints will dictate whether more than two daily keys (current and future) may be loaded in the Have Quick Radio. Such determinations are at the sole discretion of the Operational Commanders/Officers In Charge. However, the maximum key load at any time will be 6.

(3) Loaded fill devices will be stored, handled and safeguarded and TPI adhered to, when applicable in accordance with Chapter 5, Annex Z, or Annex AF, as applicable.

NOTES: 1. Issuing elements are authorized to prematurely extract paper key from its protective packaging for the purpose of downloading the key, in electronic form, to a FD. The premature extraction will be recorded on the reverse side of the corresponding CMS-25 to indicate the date of removal, reason for doing so and signature(s) of the personnel extracting the material.

2. When electronic key converted from keytape is loaded to a FD, the keytape segments can be destroyed

unless there is an operational requirement to retain them until superseded. If retained until superseded, they must be stored and accounted for in accordance with Article 775.e.(2).

3. LMD/KP-equipped accounts can store/retain electronic versions of keytape segments in the LMD/KP until superseded. (See Annex W **for authorization and reporting requirements). After loading in the LMD/KP, the hardcopy keymat segments must be destroyed, unless there is an operational requirement to retain them. If retained until superseded, they must be stored and accounted for in accordance with** Article 775.e.(2).

(4) Electronic key in a FD that is superseded during a mission will be zeroized within 12 hours of supersession. Exceptions to the 12-hour destruction standard are in Article 540.e.

(5) Upon mission completion, remaining effective key stored in a FD **will be** zeroized by LE personnel before returning the FD to the issuing element (EKMS Manager or LE). The issuing element must ensure that FDs are zeroized immediately upon their return.

(6) Issue GPS key for TAMPS electronically and retain the segments in accordance with **NOTE 2** above. During normal operations, two segments of weekly key or one segment of annual key may be issued for loading into TAMPS. If operations warrant the issue of more than two segments of weekly key, do not exceed 6 weeks' worth of key (6 segments).

(7) With the consent of the Controlling Authority, EKMS Managers or LE Issuing for units deployed are authorized to issue for subsequent loading via either a DTD or SKL up to a single edition (31 segments)of Link-16 Traffic Encryption Key (TEK) in the Multifunctional Information Distribution System Joint Tactical Radio System (MIDS-JTRS) radios.

h. **Issue and Receipt of Electronic Key in a Fill Device (FD)**:

(1) A hand receipt must be provided as a basis of receipt, inventory and reconciliation for keys issued from the LMD/KP to any FD. Maintaining hand receipts for common FDs allow for identification of the recipients as well as support

compromise recovery/notification. During the downloading process, the DTD will record information of the material being transferred which can be confirmed through a review of the audit trail data.

(2) When issued in electronic form, regardless of source (i.e. LMD/KP to the device, physical loading from a KOI-18 to a device, or device-to-device fill, local custody documents **must be used** and recipients must acknowledge receipt of the device and key (unless the device was previously issued and reflected on another local custody document).

(3) Minimum accounting information for key loaded into a fill device outside LCMS must include; the short title or designator, the edition, the reg/serial number, ALC, date of generation and/or loading, number of copies made (QTY), date of issue, the identity of issuers and recipient, classification, EKMS ID number, effective period of the key, and the serial number of the FD.

NOTE: A copy of the Controlling Authority status message can be provided to the recipients in lieu of annotating such on the local custody document. If annotated on the local custody document, the document must be properly classified in accordance with Article 715.d.

(4) Each location holding electronic key in a FD must properly safeguard and continuously account for the loaded FD by serial number, until the key is zeroized, overwritten, or otherwise destroyed.

(5) Recipients of key issued in a DTD from an LMD/KP will acknowledge receipt of the key by signing local custody documents generated by LCMS. With exception to the date of the transaction (the date the recipient signed for the material (Block 5)) and data required in blocks 14 – 16, LCMS supplies all other minimum accounting information.

i. **Issue and Receipt of Keys Stored on Removable Media (e.g., Floppy Disks, CDs)**:

(1) When keys are issued using removable media, the media will be assigned both a short title and an AL Code.

(2) Tier 0 - provided removable media such as floppy disks will have pre-assigned short titles, AL Codes, classification, and markings to indicate EKMS transactions are

on the media.

> **NOTE: Removable media containing EKMS key must be downloaded to the LMD/KP prior to issuance. Keying material contained in a Bulk Encrypted Transaction (BET) and received/stored on magnetic media, may not be directly copied by the end recipient**

(3) Locally provided removable media (e.g., floppy disks) must be assigned a short title and AL Code of 4 prior to issue. The issuing account must generate a *local* SF-153 Possession Report in LCMS to ensure the created AL Code 4 item is reflected on the Accountable Item Summary (AIS). Do not submit the "local" SF-153 Possession Report to the COR. The material is locally accountable (which means to the account and is not accountable to the COR). The short title assigned to removable media for black key will be as illustrated below:

BLACK KEY nnnnnn	(where nnnnnn = EKMS ID of the local account, and one ASCII space before "KEY" and one ASCII space before nnnnnn)

All black key removable media will be registered as AL Code 4 "COMSEC AIDS." For calendar year 2009, the edition = A, and the edition will be incremented by one on January 1st of each succeeding year. The first floppy or CD created each year will have register/serial number = 1, and each succeeding floppy/CD will increment the register by one.

As an example, an account having the EKMS ID of 170035 would register their first floppy/CD of 2009 as BLACK KEY 170035 A 1

The same account would register the 28th floppy/CD of 2009 as BLACK KEY 170035 A 28

The first floppy/CD of 2009 as BLACK KEY 170035 A 1

The 187th floppy/CD of 2009 as BLACK KEY 170035 A 187
Locally provided media will be labeled with the highest classification of the host device (e.g., LMD) and following the classification will reflect the statement "COMSEC ACCOUNTABLE" (e.g., "SECRET-COMSEC ACCOUNTABLE").

(4) A hand receipt (SF-153 LCI document) must be used to issue removable media storing keys. <u>Minimum</u> accounting guidance must include; the short title(s) assigned to the media (ensuring

issuing account’s EKMS ID is part of the short title), date of issue, and identity of issuer and recipient.

(5) Within 3 working days of receipt, EKMS key transactions stored on removable media must be uploaded to the LMD or LMD/KP, as applicable, and the media destroyed by burning or melting or returned to DIRNSA for destruction.

(6) Tier 0 - provided removable media such as floppy disks must not be copied without prior approval from the CONAUTH.

(7) Locally provided removable media must not be copied without prior approval of the issuing EKMS account.

(8) Removable media containing key are authorized for “one-time use” only (not authorized for reuse). Such media must be destroyed as indicated in subparagraph (5) above. If incineration facilities are not available, return the media to DIRNSA for destruction (See Annex S for office code/address).

(9) Loss or compromise of removable media containing key or other EKMS information must be reported as a COMSEC Incident in accordance with Chapter 9.

j. **Local Custody Issue (LCI) Limitations**:

(1) Issues to a CRF or Other Repair Facility:

(a) COMSEC equipment and related devices issued to a Crypto Repair Facility (CRF), a tender, or a maintenance pool element for repair and return must be issued using local custody procedures.

NOTE: When using local custody procedures, the material will remain on charge to the "issuing" COMSEC account and must be inventoried during account inventories in accordance with Article 766 c. (5).

(b) When COMSEC equipment will be repaired by a CRF and local custody procedures will be used, prior to pick-ups/ drop-offs, EKMS Managers must submit a message which reflects the identity of personnel authorized to drop-off or pick-up equipment for the account to the CRF.

(c) Due to the paperwork involved, account-to- account transfer procedures should only be used when it is known that the equipment will be at the repair facility for an extended period of time, or the equipment has to be shipped to the repair facility because it is located a considerable distance from the account command.

(2) Procedures to be used in the Operation of Cryptographic Equipment Exchange Program (CEEP):

AMD-9

(a) CRF San Diego is the only functioning entity under this program. CRF Norfolk and CMIO operate from authority from NCMS only for the disposition and replacement of equipment. Replacement of failed equipment can be coordinated directly from CRF San Diego without the need for formal request from NCMS under CEEP. Upon equipment failure, and prior to delivery of the failed unit, call to determine the availability of replacement equipment:

CRF San Diego COMM: (619) 556-6179 DSN: 526-6179

Once it is determined that a replacement is available, generate a SF-153 Transfer Report for the failed equipment citing this article as authority to transfer.

AMD-9

~~(a) DON users shall directly contact CMIO//N35// (757) 444-7051 ext.115 to coordinate permanent transfers of defective equipment to the Broken Copy account 078202. All such transfers must be documented on a SF-153 and will cite this article on the SF-153.~~

~~(b) CMIO will accept the defective items as a permanent transfer and replace the defective item with one from available RFI (Ready For Issue) stock, when available.~~

~~(c) If RFI assets are **NOT** available, CMIO will accept the defective item, and it will be forwarded to the supporting CRF to be screened, repaired, and returned to CMIO as maintenance operations dictate. CMIO will establish a tracking record to ensure that the first available RFI asset is returned to the customer as a permanent replacement for the item turned in.~~

~~(d) Small maintenance exchange pools are maintained at CRF Norfolk Naval Shipyard, CRF SPAWARSYSCEN San Diego and other commands reflected in EKMS 5 (series). Assets held by these commands are managed by SPAWARSYSCEN and utilized by both NCMS and CMIO as required.~~

~~**NOTE: Use of the exchange pool is not limited to "over the counter" transactions. Items can be mailed or shipped via approved methods. An item not accompanied with a SF-153 cannot be exchanged.**~~

(3) Manuals Required to Study for Advancement:

(a) EKMS accounts are authorized to issue accountable COMSEC or COMSEC-related manuals on a local custody basis to personnel of subordinate or nearby active-duty units in preparation for advancement examinations or for use in taking EKMS/COMSEC correspondence courses. Ensure that personnel are properly cleared and have facilities, if required, for storing classified COMSEC or COMSEC-related manuals.

(4) Issue to Deployed LEs of Another EKMS Account:

(a) When account holdings permit, EKMS Managers are authorized to issue material on local custody, on request, to deployed LEs of another EKMS account provided:

1. The deployed LE requesting the material is authorized to hold the material.

2. The transferring command does not reduce their holdings below the minimum necessary to meet known or reasonably anticipated requirements.

(b) Whenever possible, reproduced copies or extracts should be used.

NOTE: See Articles 781 and 784 for procedures on reproducing and extracting COMSEC material.

(5) EKMS Account Support to LEs:

(a) Occasionally, a LE command or unit will be remote from its parent EKMS Account and will also be unable to obtain necessary material as a LE from an EKMS account in the local area.

(b) Under the above circumstances, direct issue from a VDLS component (e.g., CMIO, USNDA) to the LE is permitted (after determining that the intended recipient is appropriately cleared and authorized to hold the requested material). In this situation, the LE may hold up to three months of Reserve on

Board (ROB) material.

NOTE: The procedures in this paragraph do not apply to mobile users or Navy Expeditionary Combatant Commands (NECC).

(6) Issue of COMSEC Material by a Training or School Command:

At a training or school command, local custody issue must be used to provide accountable COMSEC training and study material to authorized personnel in a training status. Recipients must be appropriately cleared, authorized, in writing access to COMSEC material and have a properly completed SD Form 572 on file with the EKMS Manager or LE Issuing, as applicable.

(7) Temporary Acceptance of Custody for LEs in Transit:

NOTE: Aviation personnel see Article 778.c.

(a) When LE personnel are in transit requiring temporary storage of COMSEC material such must be coordinated between the LE’s EKMS Manager and the EKMS account providing temporary storage.

(b) Personnel relinquishing responsibility of COMSEC material for proper storage on a temporary basis must ensure the recipients possess a clearance equal to/higher than the material being turned over for storage.

(c) LE personnel turning in COMSEC material should either; (a) lock the material in a locked comm box as described in Article 778.c.1, when possible or (b) wrap and package the material as described in Article 525.

(d) All such temporary storage requirements and the subsequent return of the material to the LE will be documented on a hand-generated LCI document.

(e) Items and/or related packages must be visually inspected upon turn-in and receipt. Signs of tampering must be reported in accordance with Chapter 9.

(f) LE personnel must ensure any superseded material is destroyed prior to turn-in for temporary storage and upon return of the material/device(s) in accordance with Article 540.

770. ISSUANCE, TRACKING AND CONTROL OF KGV-68Bs:

a. KGV-68Bs installed in missiles are considered embedded COMSEC and are accountable within the CMCS as ALC 2 items.

b. Good communications between the LE in which the KGV-68Bs are issued, the supporting EKMS Manager and the ultimate recipient are **essential.** To ensure proper accountability is maintained, it is paramount that LE personnel inform the EKMS Manager when KGV-68Bs are installed and provide the serial number(s) of the missiles in which they were installed. Typically, two KGV-68Bs are installed in each missile.

c. All issuances will be documented on a local custody document.

d. Prior to installation, LE personnel will remove the labels from the KGV-68Bs and affix them to the local custody document in which they were issued. The serial number or other unique identifier of the missile will be noted on the LCI document.

e. Following the installation, the LE personnel will provide the EKMS Manager a copy of the LCI document and the labels removed.

f. Acceptance of the responsibility for the missiles with the embedded COMSEC (KGV-68Bs) must be documented with a DD-1149 or other document to ensure continuous custody throughout the transport and acceptance of custody by the recipient.

g. A copy of the DD-1149 or other custody and shipping document will be provided to the EKMS Manager by the LE issued the KGV-68Bs. The EKMS Manager will do a Local Element Return of Physical Material for the quantity of KGV-68Bs installed and the LE will be relieved of responsibility for the quantity of KGV-68Bs installed.

h. **KGV 68Bs installed in missiles may be transferred citing this article as authorization; separate authorization from NCMS is not required.** Cite this article on the transfer SF-153 and send a copy electronically to both the recipient and Tier 1 via the X.400 message server. The remarks/comments of the SF-153 will reflect the serial numbers of the missiles in which the KGV-68Bs were installed.

Note: If multiple KGV-68Bs were previously issued to the LE on a single SF-153, the LE will retain a copy of the signed LCI return document provided by the EKMS Manager and line-out/initial the quantity on the existing SF-153 to accurately reflect the quantity still held (not installed) by the LE.

i. Upon receipt/onload of the missiles, the EKMS Manager of the unit receiving the missiles must reconcile the electronic SF-153 received and report receipt of the KGV-68Bs to the COR and the originating account.

j. EKMS Managers/Alternates will not open or attempt to open equipment with embedded COMSEC. Such will be receipted for based on the host device/equipment operating as designed in accordance with Article 758.

k. When launched/fired, the EKMS Manager of the receiving activity must ensure the required missile firing report and related Relief from Accountability report is submitted in accordance with Annex AB.

Note: Additional information can be found in the KGV-68B Security Doctrine which is NSTISSI 3003 (Section VIII).

772. SEALING COMSEC MATERIAL:

a. At the EKMS Manager or LE level, after its initial page check, unsealed COMSEC material will be sealed or resealed in accordance with the guidance contained in this article.

b. The account Manager will specify in local command instructions who (i.e., Manager or LE) has responsibility for sealing or resealing COMSEC material.

c. Unsealed COMSEC material is sealed or resealed under the following conditions:

(1) To avoid daily page checks and destruction of superseded segments (e.g., if part of an issued effective edition of extractable keying material (except keying material packaged in canisters) that will not be used for a significant period of time (e.g., two or more days)).

(2) When all segments in a canister are intentionally removed due to a packaging or production defect.

(3) When the last segment of keying material packaged in a canister (i.e., last segment of single copy keytape (segment 31 or 62) and the final copy of multiple copy segments (3/03)) is extracted for use and its effective period exceeds 24 hours.

(4) When a segment(s) of keying material is unintentionally removed from its protective packaging before its effective period.

d. Unintentional removal of key from its protective packaging prior its effective period is a non-reportable PDS in accordance with Article 1005.a.6. except when such is done in accordance with 769.g Note 1. Whether done unintentionally or intentionally to support an operational required, premature extraction MUST be recorded on the local destruction record (CMS-25) for the material.

(1) Removal of key is defined as key pulled loose from a keycard book or, in the case of canister-packaged key, segments pulled out of the canister and not detached or segments detached from the canister.

(2) The documentation of unintentional removal must include:

(a) A statement that material was unintentionally removed.
(b) Date of removal.
(c) Identity of segment(s) actually removed.
(d) Signature(s) of the individual(s) who removed the key.

(3) Key discovered removed from its protective packaging as described above before its effective period with no documentation certifying that the removal was unintentional, must be reported as a COMSEC incident in accordance with Chapter 9.

e. Intact or an entire edition of multiple copies of the **same** short title and **same** edition may be sealed in the same envelope; however, each serial/register number must be listed on the outside of the envelope when using the alternative sealing procedure in Para h.2 of this Article.

f. Sealing loose or segmented keying material of the same day's key from multiple copies or short titles in the same container or envelope is **prohibited**.

g. Only future segments, segments requiring premature extraction to support operational requirements or those as indicated in Article 772.c.3 above may be resealed. All segments superseded prior to the date the material will be sealed, must be destroyed and recorded on the destruction document of the material.

NOTE: Do not place a partially completed destruction record for segmented material inside a sealed envelope. Annotate its location on the outside of the envelope and store it with the material in a Zip Lock bag or other container.

h. **Sealing procedures**:

(1) Unsealed segmented material may be considered resealed when placed in a container (e.g., Zip Lock bag or a binder with plastic document protector pages) which will reasonably prevent the segments from being lost or misused.

(2) If the following **alternative** method is used, adhere to the following guidance:

Use an opaque (i.e., non-transparent) envelope, record the following information on the outside of the envelope:

(a) Short title.
(b) Edition.
(c) Accounting (serial/register number(s)).
(d) AL Code.
(e) Classification.
(f) Status.
(g) If material to be sealed is segmented, identify the specific segments (e.g., days 7-31, segments 10-62).

NOTE: Page check segmented material prior to placing it in an envelope.

i. When material sealed in its original production wrapper or resealed in accordance with this article is opened, the material must be page checked and all superseded segments must be removed and destroyed immediately, and the destruction recorded on the destruction record of the material.

775. COMSEC MATERIAL MANAGEMENT IN A WATCH STATION ENVIRONMENT:

a. **Watch Station Defined**: An occupied area which operates on a 24-hour, 7-day a week basis in which responsibility for all COMSEC material is transferred from the off-going to the on-coming supervisor is defined as a watch station.

NOTE: (1) For the purposes of this article, *submarines in port* are not considered watch station environments and will adhere to the inventory guidance outlined in Article 778.c.4.

(2) The provisions of 778.c.4 are NOT applicable to surface ships in port not undergoing maintenance/upkeep or where material remains issued to LEs, is accessible to duty personnel and responsibility is transferred through a daily turnover. These units will follow Article 775.

(3) To negate the need to perform watch-to-watch inventories, page checks or destruction of COMSEC material when in port for extended periods, it is recommended that Internal LEs (e.g. CIC) not maintaining communications circuits in port or at home base requiring COMSEC material turn the material in to the EKMS Manager when feasible.

b. **Custody**: All COMSEC material held or used to a watch station must be reflected on and accounted for on a watch-to-watch inventory. The LE will maintain a local custody file containing the local custody document(s) for all material issued to the LE for the duration set forth in Annex T.

c. **Responsibility**: While on duty, each watch supervisor is responsible for all COMSEC material reflected on the watch-to-watch inventory, regardless of which watch supervisor signed the local custody document for the material.

d. **Inventory Requirements**:

(1) A watch station must maintain a watch-to-watch inventory which lists all COMSEC material held (including accountability of resealed segments/material).

(2) All COMSEC material will be listed and inventoried by sighting the short title, edition, accounting number, and quantity. Equipment, which does not have an edition may be listed and inventoried by quantity only. If an equipment requiring key is operating properly the keycard/segment may be verified as present in the equipment on that basis.

(3) The inventory must be designed to provide a means of the recording dates and initials or signatures of the individuals who conducted the inventory.

(4) A complete inventory of all COMSEC material held by a watch station must be conducted whenever watch personnel change.

(5) The inventory will be conducted by appropriately cleared and authorized personnel. Watch-to-watch inventories will be signed by both the person conducting the inventory, as well as the witness.

(6) Items returned to the EKMS Manager prior to the end of the month reflected on the watch-to-watch inventory will be done using a SF-153 (Local Custody document) and lined out from the date of return on the watch-to-watch inventory and be initialed by two LE personnel. A copy of the Local Custody document signed for by the EKMS Manager and Alternate or Witness, if required will be retained by the LE turning in the material and the EKMS Manager in accordance with Annex T.

(7) Although equipment may be listed and inventoried by quantity only, LE personnel must ensure the quantity reflected on the watch-to-watch inventory is accurate. Example: If a local element was issued (3) AN/CYZ-10(V3)s but one failed and was returned to the EKMS Manager, the LE personnel must line-out, correct and initial the quantity field on the watch-to-watch inventory. The same principle applies when an increase occurs, if the watch station is issued and is accounting for (4) KG-84Cs but is issued one more, they must line-out, correct the quantity field to (5) and initial the change. Bottom line: All COMSEC material must be continuously accounted for!

NOTE: Material not reflected on a watch-to-watch inventory, which includes incorrect Short titles, reg/serial numbers or quantities for material held must be documented as a Practice Dangerous to Security in accordance with Chapter 10.

e. **Page check Requirements**: All unsealed (extracted) keying material, publications, and equipment held by the watch station must be page checked/verified in accordance with Article 757 and Annex W. Unsealed keying material includes:

(1) Keytape segment(s) that may have been

unintentionally removed from its canister before its effective period and not yet resealed in accordance with Article 772.

(2) Keytape segment(s) that cannot be destroyed immediately after use because there is an operational requirement to retain the key until it is superseded. The still-effective segment must remain under TPI if TOP SECRET, be resealed, properly stored, and accounted for until it is superseded and destroyed.

(3) Superseded extract(s) or segment(s) of keying material which is awaiting destruction, including extracts or segments which have been placed in a Special Access control container (SACC) securely welded to the interior of a GSA-approved security container.

(4) The last copy of a multiple-copy key segment which was removed from its canister and is being held until superseded. If the material will not be destroyed within 24 hours, the material must be resealed in accordance with Article 772 and added to the watch-to-watch inventory.

NOTE: Classified COMSEC related publications will be page checked and indicated as discussed in Article 757.e.4.

(5) Key in loose leaf manuals or booklet form (e.g., AKAC 874).

NOTE: Unsealed material does not include keying material packaged in canisters.

f. **Discrepancies**: Any discrepancies noted (item(s) not accounted for) must immediately be brought to the attention of the chain of command and the EKMS Manager or Alternate, as applicable prior to the off-going section being relieved and may necessitate reporting such as a COMSEC Incident in accordance with Article 945.

g. **Status Information**: Effective and supersession dates for all keying material held by the watch station must be clearly marked on the material in accordance with Article 760.

h. **Destruction**:

(1) Destruction of superseded material must be conducted in accordance with Article 790 within the timeframes set forth in Article 540.

778. COMSEC MATERIAL MANAGEMENT IN OTHER THAN A WATCH STATION ENVIRONMENT:

a. **General**: Areas where COMSEC material is required to perform a communications function and the area is not a watch station (e.g., mobile users (including CNECC), CRF, and Intermediate Maintenance Facility work-bench areas, and submarines in port) will manage COMSEC material in accordance with this article.

NOTES: 1. Mobile users or Commander, Navy Expeditionary Combat Command units include Marine Tactical units, Naval Special Warfare (SPECWAR)units, Naval Construction Battalion units, Mobile Inshore Undersea Warfare units (MIUWUs), Electronic Ordnance Disposal (EOD)units, Mobile Self Contained Command Post (MSQ) units, Mobile Ashore Support Terminal (MAST) units Mobile Integrated Command Facility Pacific (MICFAC) Units and all aircraft.

2. *When in port*, submarines will *follow* the inventory guidance in Article 778.c.4.

b. **Custody**: All COMSEC material must be issued using local custody issue (LCI) documents.

c. **Inventory Requirements**: A watch-to-watch inventory listing of COMSEC material is not required. The LCI document will serve as the record of inventory. Document completion of inventories on the front or reverse side of the local custody issue document. An inventory will be conducted in accordance with the following guidance:

(1) Aircraft:

(a) Upon change of crew personnel.
(b) Upon issue of material to aircrew personnel.
(c) Upon turn-in of material to a Manager/LE (issuing).
(d) COMSEC material will be handled as follows when end of mission results in a stop prior to returning to home airfield.

1. At a U.S. Military controlled airfield: Keying material will be stored at a near-by secure facility or will be securely stored onboard the aircraft in a security container that is mounted to or internally chained to the

aircraft structure. If the material is stored at a location other than the aircraft, place a listing of the contents inside of a protective container with the material (e.g., inside a double-locked metal box (a COMM Box), a double-locked briefcase or a double-wrapped box). Generate a hand receipt for the sealed container. On the receipt, annotate the highest classification of material placed in the container. Do not give any outward indication on the container of its contents. Obtain proper signatures on the hand receipt and provide the individual(s) storing the container with a copy of the receipt.

2. At a civilian or non-U.S. Military controlled airfield and a near-by secure storage facility will not be used or is unavailable: Securely store the material onboard the aircraft as noted above and check the aircraft and storage container every 24 hours for signs of tampering.

NOTE: If the storage container(s) on the aircraft protecting keying material are damaged or indicate evidence of possible tampering, conduct a complete inventory immediately. In the event of a discrepancy, submit a COMSEC incident report as soon as possible, in accordance with Chapter 9.

(2) Mobile Users (including CNECC forces less aircraft):

(a) Conduct an inventory of COMSEC material prior to departure and upon return to garrison (or the location where the Custodian issued the material).

(b) An inventory is not required while conducting exercises or actual operations remote from your garrison (or the location where COMSEC material is issued).

(3) CRF and Intermediate Maintenance Facility Work-bench Areas: COMSEC material held in these areas will be inventoried in accordance with Article 766 (i.e., inventory COMSEC equipment and publications annually and keying material semi-annually).

(4) LEs including submarines in port (when access to COMSEC material is not required on a daily basis; e.g., material accessed once a week for key/rekey purposes):

(a) Material need not be inventoried daily provided:

1. TPI access and handling rules are strictly

enforced.

2. The EKMS Manager is confident that proper control can be maintained for material without the need for a daily inventory and accompanying written record.

(b) LEs (*Using*) need not open security containers for the sole purpose of conducting an inventory. However, if the security container is opened for any reason and LEs (*Using*) have access to the material, an inventory will be conducted at that time and any superseded material (including that stored in electronic form) must be destroyed. LEs (*Issuing*) will comply with the destruction guidance of Article 540. Managers are encouraged to verify LEs are doing this by spot checking SF 702s.

d. **Page check Requirements**: Page check COMSEC material in accordance with Article 757 and/or any local instructions provided by the EKMS Manager.

781. REPRODUCING COMSEC PUBLICATIONS AND KEYING MATERIAL:

a. **Definition**:

(1) Reproduction of COMSEC material is the complete reproduction of an **entire** code, authenticator, call sign (CAC), publication, or keying material regardless of the reproduction method.

(2) Converting of physical keying material (ALC 1 or 4) to electronic form (ALC 6 or 7) is a form of reproduction.

(3) Reproduction of less than an entire copy of material is an extract. Handle extracts in accordance with Article 784.

NOTE: Reproduced physical material is defined as printed material (on paper) which can be duplicated by writing, typing, or electronic copying.

b. **Authority to Reproduce - Role of CO and CONAUTH**:

(1) To satisfy an operational requirement, the CO may authorize the reproduction of an entire edition of keying material. This authorization takes precedence over any restrictions or prohibitions against reproducing copies which may be contained in the Handling Instructions (HI) or Letter of

Promulgation (LOP) of the material. The CO's authority to reproduce keying material assumes the original is held by the command (i.e., command is validated to hold keying material by CONAUTH). When the keying material is reproduced for *local command use*, **do not** report reproduction outside the command unless ALC-1 material was imported into the LMD/KP. Note accountability guidelines below. When reproduced for *transfer outside the command*, the following applies:

(a) Non-emergency situation: *CONAUTH permission* ***must be*** *obtained to reproduce* ***or import*** *ALC-1 keying material for transfer to another command,* information copy to NCMS//N3//. AL Code 1 keying material reproduced for transfer outside the command must be entered into CMCS. A generation report must be submitted to the COR if ALC-1 material is imported into the LMD/KP.

(b) Emergency situation: The CO can authorize the reproduction of keying material for transfer outside of command, with after-the-fact reporting to CONAUTH, information copy to NCMS//N3//. However, the reproduction or importation of ALC 1 keying material into the LMD/KP for transfer outside the command must be entered into CMCS through submission of a possession or generation report, as applicable.

c. **Restrictions on Reproducing Keying Material**. The following keying material may **not** be reproduced:

(1) Any U.S., Allied or NATO Nuclear Command and Control Material.

(2) AKAA 285, AMSA TC 2, AMSA TX 9000, AMSA 661, AMSA 622, AMSC E/D 640, USKAC 878, USKAC 879, USKAI 4 and USKAI 5.

d. **Preparation of Reproduced Copies**:

(1) Only an original copy is authorized for use in reproducing COMSEC material.

(2) Copies may **not** be reproduced from a reproduced copy.

e. **Control of Reproduced Copies**: The CO of the command with local custody responsibility for the reproduced COMSEC material is responsible for the proper control and accountability of reproduced copies.

f. **Accountability of Reproduced Copies**:

(1) *Physical copies* reproduced from physical originals:

(a) To report the reproduction of AL Code 1 and 2 COMSEC publications and physical key (e.g., codes, authenticators, call signs) to the COR, a SF-153 Possession Report must be submitted to the COR in accordance with Article 739 and Annex T.

(b) Copies reproduced for local command use are not accountable to the COR, but must be accounted for locally and safeguarded based on the assigned classification. Do not enter copies reproduced for local command use into the CMCS.

(c) When reproduced for transfer outside the command, the preparing Manager must report their reproduction to the COR by submitting a SF-153 Possession report.

(d) AL Code 4 reproduced copies of keying material or COMSEC publications must be accounted for locally and safeguarded based on the assigned classification. These items are not be entered into the CMCS or reported to the COR.

(2) See Article 740 for guidance in accounting for physical keying material converted to electronic form for importation into the LMD/KP.

g. **Procedures to Enter Reproduced Keying Material and COMSEC Publications into CMCS**:

(1) A SF-153 Possession Report or Generation Report, as applicable must be submitted by the command that reproduced the material and

(2) The transfer of reproduced material must be documented on a TRI SF-153. The original document will be forwarded with the material and a copy must be sent electronically to both the recipient and the COR. The applicable authorization must be cited in the body of the SF-153 Transfer Report. Follow article 733.

(3) Recipients of reproduced material must prepare a TRR SF-153 in accordance with Article 742.

h. **Classification of Reproduced Copies**: Reproduced copies of COMSEC material must be assigned the same classification and special markings (e.g., CRYPTO, NOFORN) as the original material.

i. **Handling of Reproduced Copies**:

(1) Except as specified in Article 781.f.(1)(b) copies of reproduced material must be handled the same as the original material, according to classification, special marking (if any), and AL Code.

(2) Classified reproduced copies may **not** be transmitted on line, and may not be disassembled for wider distribution.

(3) Unclassified reproduced copies may be disassembled for wider distribution only within the command.

j. **Assignment of Short Titles and Accounting Data**: LCMS provides the Manager the choice of supplying a short title for key imported in the KP or allowing LCMS to assign the short title. Due to the availability of both paper and electronic versions of the same short title during the physical to electronic transition (PET), there should be little need to supply an electronic copy for transfer outside the command. The Manager must assign the original short titles/accounting information when hard-copy AL Code 1 keying material is downloaded into the LMD for the sole purpose of obtaining a copy. The prefix letters that precede the accounting number in the short title field must also be entered (e.g., USKAK 9999 (AB)). The preparing EKMS Manager or Alternate will assign short title/accounting data to all reproduced copies in accordance with the following procedures:

(1) Except as specified in Article 781.f.(1)(b), the same short title (including any edition suffix), classification, and AL Code of the original material will be assigned to each reproduced copy.

(2) Assignment of accounting numbers to AL Code 1 and 6 reproduced copies, together with the four digit suffix, as described in NOTE below, will be used to assign an accounting number to reproduced copies.

NOTE: If the accounting numbers contain more than four digits, use only the last four digits of the original accounting number. A four-digit suffix beginning with 001 will then be appended to each reproduced copy along with the original accounting number in a one up sequence as described below.

EXAMPLE: If 30 copies are to be reproduced from USKAK 9999 EE accounting number 123456, the short title and accounting number of the first reproduced copy would be "USKAK 9999 EE 3456001." The second reproduced copy would be "USKAK 9999 EE 3456002," and so on.

k. **Listing Reproduced Copies on Accounting Documents**:

(1) Each individual reproduced copy of AL Code 1 material must be reflected on a separate line of an account document.

(2) Both ALC 2 and 4 material are accountable by quantity and not by reg/serial number. Accordingly, reproduced AL Code 2 and 4 material will be listed as a single line entry with the total quantity listed in the quantity column/field of the accounting document.

l. **Local Custody Requirements for Reproduced Copies**: Local custody requirements for reproduced copies are the same as for original copies.

784. PREPARING EXTRACTS FROM COMSEC PUBLICATIONS AND KEYING MATERIAL:

a. **Definition**:

(1) An extract is defined as a portion or segment of a COMSEC publication or keying material.

(2) An extracted portion or segment is physically separate from the material from which it is prepared, either as a result of physical removal, manual reproduction (i.e., writing, typing, or electronic copying), or conversion to electronic form.

(3) References to, or statements revealing the main point of a paragraph, an article, or a section of a publication are not extracts, nor are brief quotations used in correspondence or messages.

(4) Extracts may be issued on a local custody document to another EKMS account only when the recipients account is authorized to hold the material or when required for use within the command extracting the material.

b. **Authority to Prepare Extracts**:

(1) Emergency situation: To satisfy an emergent operational requirement, the CO may authorize the preparation of extracts from any COMSEC material authorized to be held by the account.

NOTE: This authorization is applicable to both unclassified and classified material and takes precedence over any restrictions or prohibitions against extracting material which may be contained in the Handling Instructions (HI) or Letter of Promulgation (LOP) of the material involved.

(2) Classified Extracts in a Non-emergency situation:

During non-emergency situations, the following sources constitute authorization for preparing classified extracts:

(a) LOP, Handling Instructions, forward page, or text of the publication.

(b) Separately promulgated directive affecting a series of publications.

(c) Controlling Authority of the material when the above sources do not address extraction.

(3) **Unclassified Extracts in a Non-emergency situation**:

During a non-emergency situation, in the absence of specific directives to the contrary, this article constitutes authorization to prepare extracts of unclassified material regardless of the overall classification of the publication.

(4) **Special Authorization for Training and School Commands**:

(a) Service schools and training commands are authorized to make extracts of classified information from any COMSEC material authorized to be held by the command for training purposes only.

(b) Extracts may not be removed from the school or training command, and shall be accounted for and destroyed locally.

c. **Controlling Classified Extracts**:

The CO of the command with local custody responsibility for the extracts is responsible for the proper control and safeguarding of classified COMSEC extracts.

d. **Classification of Extracts**:

Extracts from classified COMSEC material will be classified and assigned any applicable special markings (e.g., CRYPTO, NOFORN) in accordance with the following procedures:

(1) If individual paragraphs or other subdivisions of a classified publication are not assigned a classification and special markings, and if no classification guidance is included in the publication itself, the extract shall be assigned the same classification and special marking as that of the overall publication.

(2) If individual paragraphs or other subdivisions of a classified publication are assigned a classification and special markings, the extracts shall be assigned the classification and special markings as the paragraph or section from which the extracts are made.

e. **Disassembling COMSEC Publications**:

(1) To permit wider dissemination only within a command, the CO may authorize the EKMS Manager or LE, to make a temporary subdivision of an unclassified COMSEC publication.

(2) Classified COMSEC publications may not be disassembled for dissemination.

f. **Local Custody Requirements**:

(1) Extracts of COMSEC keying material marked CRYPTO will be documented on local custody forms in accordance with Article 769.

(2) Extracts of other COMSEC material, including keying material not marked CRYPTO, do not have to be documented on local custody forms. This material must be handled and accounted for based on its assigned classification in accordance with SECNAV M5510.36.

g. **Return of Defective Extracts to NSA**:

(1) If specifically authorized by NSA, defective extracts will be forwarded to NSA on a SF-153 as a local custody issue.

(2) Do not assign a TN to the SF-153 and do not send a copy of the SF-153 to NCMS.

(3) Retain your copy of the SF-153 for accountability documentation.

h. **Destroying and Documenting Destruction of Extracts**:

(1) Extracts of COMSEC keying material marked CRYPTO shall be destroyed in accordance with Article 540.

(2) Extracts from other COMSEC material shall be destroyed based on their assigned classification in accordance with SECNAV M5510.36.

(3) Destruction of COMSEC material extracts will be recorded on local destruction documents in accordance with Article 736.

(4) Use a local custody document to account for defective extract(s) of COMSEC material returned to NSA.

(5) Attach a copy of the local custody document to the local destruction record to account for an extract(s) returned to NSA when completing the destruction document for the entire edition.

NOTE: For keys stored in a DTD or SKL see Annex Z or Annex AF, as applicable.

787. ENTERING AMENDMENTS AND CORRECTIONS TO COMSEC PUBLICATIONS:

a. **General**:

(1) Amendments and corrections are permanent changes to COMSEC and COMSEC-related publications (hereinafter referred to as publications) which incorporate updated information. Amendments and corrections to publications contained on CD-ROM will be issued in paper-based form and must be stored/retained with the CD.

(2) Actions based on outdated or incorrect information

have the potential to adversely impact operational missions and administrative procedures. Therefore, amendments and corrections to publications must be entered only by properly trained and authorized personnel.

(3) The EKMS Manager must ensure that written guidance, based on the procedures detailed in this article, is provided to all personnel entering amendments and corrections to publications.

(4) Changing a publication on the basis of an apparent discrepancy is not authorized. Changes to publications may be entered only as authorized by the publication's originator.

(5) Figure 7-4 is a check-off list which may be reproduced for use in entering changes to COMSEC material and COMSEC-related publications and Figure 7-5 is an example Certification of Amendment Entry form.

b. **Types of Amendments**:

(1) Printed Amendments:

(a) Printed amendments may consist of replacement pages, cut-out inserts, pen-and-ink changes, or any combination thereof.

(b) Printed amendments are, normally, distributed via the CMIO or directly from NCMS.

(2) Message Amendments:

(a) Message amendments normally consist of only pen-and-ink changes.

(3) Corrections to Amendments:

(a) Corrections to amendments are permanent alterations to printed or message amendments.

(b) Corrections may be printed or they may be issued as a message. Normally, the next printed amendment or message amendment will incorporate the information issued in a correction.

c. **Numbering of Amendments and Corrections**:

(1) All amendments to a basic publication are numbered consecutively while corrections to amendments are not numbered.

(2) Amendments and corrections to amendments must be recorded on the Record of Amendments (ROA) page of the publication. For example, the record of amendments and corrections to amendments entered in a specific publication could appear as follows: (printed) Amendment 1, (printed) Amendment 2, (message) Amendment 3, (Printed) Correction to Amendment 3.

(3) Amendments must be entered sequentially. For example, Amendment 4 may not be entered before Amendment 3 has been entered. In the event more than one correction to the same amendment is received, the corrections should be entered according to the date of promulgation.

d. **EKMS Manager Actions**:

(1) Upon receipt, promptly review amendments and corrections and promulgate any significant information to appropriate command personnel.

(2) Amendments and corrections will be entered as directed by originator.

(3) EKMS Managers who transfer AL Code 4 publications to another EKMS account must forward all amendments or corrections to the command(s) holding the basic publication for a period not to exceed 90 days. Thereafter, the recipient must coordinate with the CONAUTH to ensure receipt of future amendments.

e. **Supply of Amendments**:

(1) NCMS and the servicing VDLS component are responsible for supplying the command with printed amendments and corrections. However, the EKMS Manager is responsible for ensuring that a publication contains the most current amendment. Status documents (e.g., SCMR) are the most up-to-date sources for determining the latest amendment to a COMSEC publication.

(2) Request disposition instructions from the originator for excess or unneeded copies of classified, accountable printed amendments and corrections. Ensure that the authorization for either the destruction and/or transfer is annotated on the SF-153 Transfer or destruction report as applicable.

(3) Excess or unneeded copies of unclassified, non-accountable amendments and corrections may be destroyed at the discretion of the Manager.

f. **Local Custody**:

Local custody issue of AL Code 1 or 2 printed amendments and corrections must be documented on an appropriate local custody document.

g. **Entering Amendments**:

(1) Instructions:

(a) Each amendment provides instructions on the status or effective date of the amendment and step-by-step procedures for entering the amendment (e.g., specifically identifying which pages are to be removed from the basic publication and which pages from the amendment are to be added, and/or pen-and-ink corrections).

NOTE: Amendment instructions must be read and clearly understood prior to entering an amendment.

(b) Pen-and-Ink Changes:

1. Only **black or blue/black ink** will be used to make pen-and-ink corrections. No other color of ink may be used.

2. Pen-and-ink corrections must be identified, in the margin, opposite their entry (e.g., Amend 5, Correction to Amend 5).

(c) Printed Changes:

1. Effective amendments must be promptly entered and verified as soon as possible after receipt.

2. An amendment effective in the future should be entered as close to its effective date as possible. If an amendment is entered substantially before its effective date, annotate "Effective (date)" in the margin of each replacement page and opposite each pen-and-ink change.

(2) Recording the Entry:

(a) The individual entering the amendment must sign and date the ROA page of the publication certifying that he/she entered the change.

(b) The identity of the change (e.g., Amendment 1 or Correction to Amend 1) and, if applicable, the ALCOM number and/or Date-time-Group (DTG) of the message must be recorded on the ROA page in order to properly identify the change.

(3) Entering Amendments in Sealed Publications:

If a sealed publication is opened to enter an amendment or a correction, the publication should be resealed after verification of the change and page checking the publication (if required).

(4) Page check of Publication and Amendment Residue:

(a) Conduct a page check of publications and amendment residue in accordance with Article 757 and Annex V. Ensure that the publication's Record of Page checks (ROP) page is annotated.

(5) Verifying Proper Entry of an Amendment:

(a) The entry of amendments must always be verified by a second individual, who may be properly cleared and authorized person.

(b) The person verifying an amendment entry must certify, by placing their initials in the margin alongside the amendment entry on the ROA page, that it was entered correctly and that the signature, date, and amendment identification have been entered on the ROA page of the basic publication.

NOTE: Initialing the ROA page entry is sufficient for verifying an amendment entry. A separate entry is not appropriate since the verifying individual did not actually enter the amendment.

(c) As a part of the verification process, the person verifying entry of an amendment must conduct a second page check of the basic publication and the amendment residue if the amendment removed, substituted, or added pages. This second page check of the basic publication must be recorded (i.e., signature and date) as a separate entry on the ROP Page.

NOTE: The list of amendment residue, normally found at the end of the amendment instructions, must be used in page checking the amendment residue. The verifying individual must indicate this second page check of the residue by initialing and dating the front page of the amendment residue.

h. **Destruction of Amendment Residue**:

Destruction of amendment residue may be verified in one of two ways at the option of the EKMS Manager.

(1) The LE who signed the local custody document for the amendment can furnish the EKMS Manager with a local destruction record and certification of proper entry and verification (see last page of this chapter); **OR**

(2) The EKMS Manager can personally verify the entry by the LE, destroy the residue, and return the basic publication to the LE.

NOTE: Classified and unclassified amendment residue must Be destroyed as soon as possible but no later than five working days after an amendment entry.

i. **Recording Destruction of Amendment Residue**:

(1) Document destruction locally and maintain required records in accordance with Article 736.

(2) The destruction of unaccountable, classified amendment residue will be conducted in accordance with SECNAV M5510.36. Do not report destruction to the COR or NCMS.

790. PROCEDURES FOR DESTROYING COMSEC MATERIAL IN PAPER FORM:

a. **General**:

(1) EKMS Managers must ensure that all personnel who destroy COMSEC material follow the destruction criteria, reporting, methods, procedures and documentation requirements set forth in this manual.

(2) Attention to detail when destroying COMSEC material cannot be overstressed. Failure to follow proper procedures is one of the principle causes of both COMSEC incidents and Practices Dangerous to Security.

(3) Keying material marked or designated CRYPTO is the most sensitive item of COMSEC material. Therefore, the immediate, complete, and proper destruction of superseded keying material is of the highest importance.

(4) **Prior** to destroying any COMSEC material, verify, validate, and sight each item of material to be destroyed.

(5) The two individuals destroying COMSEC material are **equally responsible** for the timely and proper destruction of the material and the accuracy of the destruction document(s).

(6) Destruction criteria (i.e., timeframes and authorized methods) are contained in Chapter 5. Reporting and documentation requirements are detailed in Article 736. The information below details the steps to be followed by all personnel when destroying COMSEC material.

b. **Verifying Status Information**:

(1) The individuals conducting destruction of COMSEC material must ensure that the material to be destroyed is in fact superseded and/or authorized for destruction prior to actually destroying the material.

(2) EKMS Managers are responsible for ensuring that correct and the most up-to-date status information for COMSEC material is provided to personnel destroying COMSEC material **(this includes verifying status markings applied to the material is accurate at the time of issue)**

c. **Verifying Short Title and Accounting Data**:

(1) To accurately verify the material being destroyed against the destruction document, the individual responsible for destruction must read the short title(s), edition, register/serial number and the segment number of the material being destroyed to the EKMS witness.

(2) The EKMS witness must verify the accuracy and completeness of the entries on the destruction document.

(3) The EKMS witness must then read the short title(s), edition, register/serial number and the segment number to the individual responsible for destruction who then verifies the accuracy and completeness of the entries on the destruction

document against the information read by the witness (second person).

NOTES: (1) If both personnel destroying the material are not in agreement that the material is superseded and authorized for destruction STOP! Superseded material must be destroyed within 12 hours of supersession therefore, if in doubt, there is no reason to go ahead with the process. (See Note 3 below)

(2) If any of the information read off from the material (Short Title, Edition, Reg Number, Segment/Copy) does not match that reflected on the destruction document especially when other segments have already been destroyed STOP! (See Note 3 below)

(3) Contact the EKMS Manager, an Alternate, or LE Issuing, as applicable for assistance.

d. **Timeliness of Destruction**:

The two individuals destroying COMSEC material must ensure the superseded material is destroyed within the timeframes specified in Chapter 5.

e. **Security Safeguards**:

The two individuals responsible for destroying COMSEC material must strictly observe the following security safeguards when the use of burn bags or other containers is required due to a large quantity of material being destroyed.

(1) Sealing and Marking Destruction Containers:

After verifying the material to be destroyed against the destruction record, place the material in burn bags or other destruction containers, seal them securely, and mark the containers to identify them as containing COMSEC material. In addition, the containers must be numbered to reflect the total number of containers (e.g., 1 of 3, 2 of 3, 3 of 3).

(2) Separation and Control of Destruction Containers:

(a) Keep all destruction containers which contain unshredded COMSEC material separate from all destruction containers containing non-COMSEC material.

(b) Until they are physically destroyed by an authorized method, destruction containers containing COMSEC material must be afforded the same security and storage protection required for the COMSEC material itself. For example, destruction containers containing strip-shredded COMSEC material must be protected based on the highest classification of the shredded material contained therein. Destruction containers containing cross-cut shredded microfiche material must be protected based on the highest classification of the material. Guidance specific to Paper-Mylar-Paper (PMP) COMSEC materials can be found in Chapter 5.

NOTE: Depositing superseded COMSEC keying material segments or extracts into a burn bag, a SACC or other locked container does not constitute physical destruction. If a special access control container (SACC) is used, all deposited superseded keying material must be destroyed within the timeframes specified in Chapter 5.

(3) Transportation of Containers:

Transport destruction containers directly from the secure area to the area in which physical destruction will take place. Attending to other business or to personal matters while enroute to the destruction site is strictly prohibited.

f. **Witnessing Destruction**:

(1) The two individuals conducting destruction of COMSEC material must **not** complete (i.e., sign and date) destruction documents until after the material has actually been destroyed. Therefore, the two individuals conducting the destruction must personally witness the complete destruction of the material.

(2) In the case of large destruction facilities (e.g., disintegrators), operated for the benefit of commands in the area, the destruction containers may be given to the individual(s) who are operating the destruction facility.

NOTE: If a discrepancy in a COMSEC material destruction container is noted prior to the physical destruction of the container (e.g., inaccurately numbered, missing or broken container) and if the nature of the container discrepancy causes any doubt whatsoever about the accuracy of the corresponding destruction document(s), then the contents of all containers involved must be removed and re-verified.

g. **Inspecting Destruction Devices and Destroyed Material**:

(1) When an incinerator is used for destruction, ensure that the flues are properly screened and secured to prevent possible escape of partially burned material.

(2) The two individuals conducting destruction must monitor the entire destruction process and inspect the destruction device and the surrounding area afterward to ensure that destruction was complete and that no material escaped during the destruction process. These procedures apply to all destruction devices discussed in Chapter 5.

(3) The residue from destroyed material must be inspected to ensure that the destruction was complete (i.e., no unburned and readable bits of material remain).

(a) In the case of shredders, choppers, and pulverizers (dry process), and pulpers and disintegrators (wet process), only a representative sample of the residue needs to be examined to ensure that the device was working properly.

(b) In the case of ash residue from an incinerator or other method of burning, the ashes must be inspected and, if necessary, broken up by carefully stirring or sifting, or be reduced to sludge with water.

792. DESTRUCTION OF COMSEC MATERIAL IN ELECTRONIC FORM

1. Editions of keying material held in electronic form have the same effective and supersession dates as that of the physical version of the Short Title. Example: USKAT 1148 edition A and USKAD 1148 edition A would both be effective on and supersede on the same date. EKMS Managers should verify that editions of Short Titles received in electronic form do NOT have different effective/supersession dates than the physical version of the same material (when held).

2. The destruction of unissued keying material held in electronic form at the account level does not require a witness and is accomplished through the “Direct Destruction of Own Electronic Key” discussed in EKMS-704(series).

3. Traditional electronic key issued to a Local Element (LE) will be reflected on the working copy of the end of the month destruction reported generated by the EKMS Manager for the

LE.

4. Modern key issued to the LE such a keying material used for Secure Data Network Systems (NES) or Iridium phones must be documented by the LE on a locally-generated destruction report following loading. The serial number of the device in which the key was loaded will be reflected in Block 13 (the remarks block) of the local destruction report.

5. Upon receipt of the signed destruction document from the LE, the EKMS Manager must remove the item from LCMS through the use of the "Record Filled In End Equipment" function in LCMS. Failure to do so will result in the material still be reflected on the Accountable Item Summary and result in a non-reportable PDS (late-destruction) when such is not done NLT the 5th working day of the month following use of the material.

NOTE: When either "Direct Destruction of Own Electronic Key" or "Record Filled in End Equipment" is used, a working copy of a destruction report will not be produced/generated in LCMS. However, the material will appear on the next consolidated destruction report dependent upon the ALC of the material.

6. When modern key which has a unique Key Management Identifier (KMID) is issued to and stored in a DTD or SKL if the keying material was not loaded and reported previously to the EKMS Manager as "Filled in End Equipment" should the DTD or SKL become corrupted, the LE MUST generate a destruction report and provide it to the EKMS Manager. Modern key cannot be reissued or returned in LCMS. **Failure to follow this guidance will result in a COMSEC incident in future inventories as the key will still be charged to the account.**

793. U.S. ARMY AND AIR FORCE COMSEC ACCOUNTS:

When corresponding with an Army or Air Force COMSEC account, the COR of that service must be an information addressee on all correspondence (e.g., letter, message). COR addressees are contained in Annex S.

CONFIDENTIAL (When Filled In)

CMS-25/ONE-TIME KEYING MATERIAL DESTRUCTION REPORT

Retain this form locally IAW Annex T, EKMS 1(series). See Article 790 for instructions on destroying one-time keying material. These individual one-time keying material cards or segments were destroyed on the dates and by the two individuals indicated below:

SEGMENT	**DATE EXTRACTED**	**DATE DESTROYED**	**SIGNATURE**	**SIGNATURE**
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				
31				

(Command Title and Account Number)

Short title/Edition:_________ Reg#/Accounting#:__________ AL Code:_______
For destruction of the entire publication IAW EKMS 1(series) on TN_______
dated___________
Grade/Signature______________________ Grade/Signature______________________
Derived from: EKMS 1(series)
Declassify on: DD Month YYYY

CONFIDENTIAL (When Filled In)

Figure 7-1

Explanation of Key tape Crypto Periods When to Change

First Letter	# of Keys	# of Copies	Total Segments	Second Letter	Crypto Period
A	31	1	31	A	Daily (24hrs)
B	5	3	15	B	Weekly (7days)
C	1	5	5	C	Monthly
D	6	5	30	D	Special (24hrs)
E	5	1	5	E	No Prescribed period
F	1	10	10	F	Three months
G	16	1	16	G	Yearly
H	1	31	31	H	Contact CONAUTH
I	1	15	15	I	Six months
J	26	1	26	J	Monthly (Beginning 1st day used)
K	6	12	72		
L	35	1	35		
M	2	1	2		
N	CONTACT	CONTROLLING	AUTHORITY		
P	1	45	45		
Q	34	1	34		
R	4	5	20		
S	75	1	75		
T	12	1	12		
U	65	1	65		
V	62	1	62		
W	1	65	65		
Y	26	2	52		
Z	15	5	75		

```
 ________________________________________________________________________
 _      ___________________________________________________________      _
 _    \          SECRET          CRYPTO      NOFORN            \         _
 _    /          USKAK      ED    REG NO      SEG              /         _
 _    \__________________________________________________________\       _
 _    /       AA          XXXXXX      XX     X                 /         _
 _    \__________________________________________________________\       _
 _     CRYPTO PERIOD   SHORT TITLE   ED   REG NO    TAPE SEG             _
 _                                                                       _
 ________________________________________________________________________
```

NOTE: See Figure 2-1 for additional explanation of Crypto Keying Periods

Derived from: EKMS 1(series)
Declassify on: DD Month YYYY

CONFIDENTIAL (When Filled In)

FIGURE 7-1-2

CMS 25 ONE-TIME KEYING MATERIAL DESTRUCTION REPORT

1. Purpose: The CMS 25 COMSEC keying material report is a two-sided document used to record destruction of individual, one-time keying material segments of COMSEC material. Side one is numbered 1-31. The reverse side provides an explanation for the digraphs that are printed to the left of the short title on each segment of extractable tape.

2. Preprinted CMS 25 Reports: The current version of the CMS 25 (revised date of 11/82) or a locally prepared equivalent form may be used.

3. Date of Extract: This column is used to record the actual date an individual segment of extractable COMSEC keying material is extracted from its protective packaging. The use of this column is optional.

4. Signatures: The two individuals conducting destruction shall affix their signatures or initials directly opposite the segment being destroyed. The use of lines or ditto marks to connect signatures or initials is **prohibited**.

5. Date of Destruction: The actual date of destruction must be entered opposite the two sets of signatures or initials. The use of lines or ditto marks to connect dates is **prohibited**.

6. Account/Short Title Date: The complete short title, edition, register or serial number (if applicable), and AL Code must be annotated on the bottom of this report.

7. Improperly Completed Form: The lack of two signatures or sets of initials and a date of destruction for each copy of segmented material destroyed is a PDS. The absence of or lack of a complete short title, edition, register/serial number and AL Code constitutes a PDS. Handle PDSs in accordance with Chapter 10.

8. Restrictions on Use: When the CMS 25 or a locally prepared equivalent form is used, the destruction of one and only one copy of a short title may be recorded on the report.

FIGURE 7-1-3

CMS 25B COMSEC KEYING MATERIAL LOCAL DESTRUCTION REPORT

The individuals whose signatures appear below, certify that they have destroyed the individual keytape segments on the dates indicated. Retain this form in accordance with Annex T.

CONFIDENTIAL (When Filled In)

SEGMENT	**SIGNATURE**	**SIGNATURE**	**DATE OF DESTRUCTION**
1A			
2A			
3A			
4A			
5A			
6A			
7A			
8A			
9A			
10A			
11A			
12A			
13A			
14A			
15A			
16A			
17A			
18A			
19A			
20A			
21A			
22A			
23A			
24A			
25A			
26A			
27A			
28A			
29A			
30A			
31A			

____
(Command Title and Account Number)

____________ ________ __________ __________
SHORT TITLE EDITION REG NO AL CODE

Derived from: EKMS 1(series)
Declassify on: DD Month YYYY

CONFIDENTIAL (When Filled In)

FIGURE 7-2

CMS 25B COMSEC KEYING MATERIAL LOCAL DESTRUCTION REPORT

The individuals whose signatures appear below, certify that they have destroyed the individual keytape segments on the dates indicated. Retain this form in accordance with Annex T.

CONFIDENTIAL (When Filled In)

SEGMENT	**SIGNATURE**	**SIGNATURE**	**DATE OF DESTRUCTION**
1B			
2B			
3B			
4B			
5B			
6B			
7B			
8B			
9B			
10B			
11B			
12B			
13B			
14B			
15B			
16B			
17B			
18B			
19B			
20B			
21B			
22B			
23B			
24B			
25B			
26B			
27B			
28B			
29B			
30B			
31B			

____
(Command Title and Account Number)

___________ SHORT TITLE ________ EDITION ________ REG NO _______ AL CODE

Derived from: EKMS 1(series)
Declassify on: DD Month YYYY

CONFIDENTIAL (when Filled In)

FIGURE 7-2-1

CMS 25B COMSEC KEYING MATERIAL LOCAL DESTRUCTION REPORT

1. Purpose: The CMS 25B is a two-sided document used to record destruction of keytape segments of COMSEC keying material packaged in the "VF" format (62 unique segments per canister). The destruction of segments 1-31A shall be recorded on the "A" side. Segments 1-31B on the "B" side. Complete information must be recorded on both sides when this form is used.

2. Signatures: The two individuals conducting destruction shall affix their signatures or initials directly opposite the segment being destroyed.

3. Date of Destruction: The actual date of destruction must be entered opposite the two sets of signatures or initials.

4. Account/Short Title Data: The EKMS account number of the issuing account must be annotated on the CMS 25B in addition to the complete short title, edition, register or serial number (if applicable), and the AL Code. LEs of a command other than the issuing command must annotate their command title vice the title of the issuing command.

5. Improperly Completed Form: The lack of two signatures or sets of initials and a date of destruction for each copy of segmented material destroyed is a PDS. The absence of or lack of a complete short title, edition, register/serial number, and AL Code constitutes a PDS. Handle PDSs in accordance with Chapter 10.

FIGURE 7-2-2

CMS 25MC COMSEC KEYING MATERIAL LOCAL DESTRUCTION REPORT

The individuals whose signatures appear below, certify that they have destroyed the individual keytape segments on the dates indicated. Retain this form in accordance with Annex T.

CONFIDENTIAL (When filled in)

Seq/Copy #		**Signature**	**Signature**	**Date of Destruction**
1/01				
1/02				
1/03				
1/04				
1/05				
2/01				
2/02				
2/03				
2/04				
2/05				
3/01				
3/02				
3/03				
3/04				
3/05				

(Command Title and Account Number)

____________	__________	__________	_____________
SHORT TITLE	**EDITION**	**REG #**	**AL CODE**

Derived from: EKMS 1(series)
Declassify on: DD Month YYYY

CONFIDENTIAL (When filled in)

FIGURE 7-3

CMS 25MC COMSEC KEYING MATERIAL LOCAL DESTRUCTION REPORT

1. **Purpose**: The CMS 25MC is used to record destruction of multiple copy segments (i.e., 1/01, 1/02, 1/03, etc.) of COMSEC keying material packaged in canisters.

2. **Signatures**: The two individuals conducting destruction must affix their signatures or initials in the signature blocks directly opposite the specific copy of the segmented keying material being destroyed.

3. **Date of Destruction**: The actual date of destruction must be annotated in the date of destruction block.

4. **Account/Short Title Data**: The EKMS account number of the issuing account command, the complete short title, edition, register or serial number (if applicable), and the AL Code must be annotated on this form. LEs of a command other than the issuing command must annotate their command title vice the title of the issuing command.

5. **Improperly Completed Form**: The lack of two signatures or sets of initials and a date of destruction for each copy of segmented material destroyed is a PDS. The absence of or lack of a complete short title, edition, register/serial and AL Code constitutes a PDS in accordance with Chapter 10.

FIGURE 7-3-1

CHECK-OFF LIST FOR ENTERING AMENDMENTS TO PUBLICATIONS

Initial Each Item When Completed

Person Entering Amendment (Initial)   Person Verifying Entry (Initial)

1. Instructions for entering the change have been read and understood. _______ _______

2. Black or blue-black ink only used for deletions and pen-and-ink changes. _______ _______

3. Prepared cutouts used. Locally-typed cutouts identify change being entered (e.g., Amend 1). _______ _______

4. Information superseded by a cutout deleted in ink before cutout affixed. _______ _______

5. Flaps used only if there is no room to affix cutout flat on page. _______ _______

6. Each pen-and-ink change is identified by amendment number or correction to a specific amendment. _______ _______

7. For change entered substantially before its effective date, "Effective (date)" notation marked in margin on all pages where change was made. _______ _______

8. Record of Amendments page completed and signed by the person entering the change and initialed by the person who verified the entry. _______ _______

9. If change removed, added, or substituted pages, publication page checked and the Record of Page checks page signed and dated by person who entered the change and the person who verified the change. _______ _______

10. If residue from change is more than one page, page check of residue made and residue initialed or signed and dated by the person who entered the change and the person who verified the change. _______ _______

11. Residue of change entered by LE was destroyed. Date of destruction and signatures of the two people who destroyed the material recorded on local destruction record, and record forwarded to the Manager. _______ _______

_____________________________ (Date and signature of person who entered the change)

_____________________________ (Date and signature of person who verified the change)

FIGURE 7-4

EXAMPLE OF CERTIFICATION OF AMENDMENT ENTRY

MEMORANDUM

____
(date)

From:
To: EKMS Manager

Subj: CERTIFICATION OF AMENDMENT ENTRY, VERIFICATION, AND LOCAL DESTRUCTION OF AMENDMENT RESIDUE

Ref: (a) EKMS-1(series) Article 787

Encl: (1) Check-off List For Entering Amendments to Publications

1. In accordance with reference (a) and enclosure (1), on (date), Amendment ______, accounting number _____, was entered into (publication short title and edition), EKMS ID _____.

2. Proper entry of the amendment was verified as indicated in enclosure (1).

3. The residue of the amendment was properly destroyed on (date) by the two individuals whose names and signatures appear below:

_____________ Printed Name	____________ Printed Name
______________ (Signature)	______________ (Signature)

FIGURE 7-5

CHAPTER 8 -- DISESTABLISHMENT AND COMMAND-TO-COMMAND TRANSFER OF AN EKMS ACCOUNT

CHAPTER 8 - DISESTABLISHMENT AND COMMAND-TO-COMMAND TRANSFER OF AN EKMS ACCOUNT

801. REQUIREMENT TO DISESTABLISH AN EKMS ACCOUNT:

a. An EKMS account must be properly disestablished whenever the command is being decommissioned, deactivated, or no longer requires an EKMS account. The requirement to disestablish an EKMS account will be validated by the action addressees indicated in Article 810 via official message to NCMS.

b. The provisions of this chapter applies to EKMS accounts. The parent EKMS account must provide guidance and direction to Local Element (LE) personnel when an account will be disestablished.

c. Early communications and notification to external LE's by accounts which are disestablishing is essential to minimize or prevent mission impact to the LE. This includes planning and assistance in identification of a possible source account which may be able to provide the support as well as ensuring materials required by the LE is brought to the attention of the gaining EKMS Manager to ensure timely submission of any allowance modifications required to mitigate potential mission impact.

d. Should support not be available from another account in the area when a supporting account is disestablished, the LE must discuss the matter, the timeframe and their COMSEC requirements with their Immediate Superior in Command (ISIC) to determine if the LE's organization should establish their own COMSEC account.

805. INVENTORY REQUIREMENT FOR DISESTABLISHMENT:

a. **All** regularly required inventories (ie, SAIR, CCIRs, etc…) will be conducted and reconciled as required in accordance with Article 766. Accounts working towards disestablishment are not exempt from any inventories identified in Article 766.

b. The account **must be 100 percent reconciled** NLT 30 calendar days prior to the requested disestablishment date.

810. DISESTABLISHMENT PROCESS:

a. **Request to Disestablish Message**: A request to disestablish an EKMS account must be submitted via official message a minimum of **120** days prior to the disestablishment date being requested. Messages must be addressed as indicated in the matrix below.

Required PLA's for Disestablishment Requests

	USCG	**USMC**	**USN & MSC**	**Official Reserve Commands**
UNITS ADMINISTRATIVE & op COC	I	I	I	I
CMC C FOUR CY WASHINGTON DC	NA	A	NA	NA
CMIO NORFOLK VA	I	I	I	I
COMLANTAREA or COMPACAREA COGARD	I	NA	NA	NA
TYPE/FLEET COMMANDER (TYCOM/FLTCDR)	NA	NA	A	NA
COGARD C4ITSC ALEXANDRIA VA//BOD-IAB//	A	NA	NA	NA
COMMARCORSYSCOM QUANTICO M C THREE	NA	I	NA	NA
COMNAVRESFOR NORFOLK VA	NA	NA	NA	A
COR	I	I	I	I
ISIC	I	I	I	I
NCMS WASHINGTON DC	I	I	I	I
SERVICING DCS STATION	I	I	I	I
SPAWARSYSCEN ATLANTIC CHARLESTON SC	I	I	I	I
SERVICING CMS AA TEAM	I	I	I	I

b. **NCMS Action**: Upon receipt of approval via official message by the applicable action addressees, NCMS will:

(1) Request date to suspend account in Tier-1 from account.

(2) Once suspension date is received, notify CMIO to terminate auto distribution, and suspend account in Tier-1.

(3) Concurrently, provide equipment disposition messages and work with the account to resolve IRST discrepancies.

(4) Continue reconciliation of required inventories in accordance with Annex AF that may occur during the disestablishment process.

(5) Once the account has submitted a COAL to Tier-1 reflecting zero holdings, access the associated IRST and work with the account to resolve any remaining discrepancies.

(6) Once all required inventories have been reconciled, and any unresolved discrepancies have been corrected, request the Final Disestablishment Report from the account.

AMD-9

(7) Upon receipt of the Final Disestablishment Report, verify all required actions have been completed; send a Final Record Clearance message to the account's command, the ISIC, and the servicing ~~CMS A&A~~ COR Audit Team; and change the account status in Tier-1 to, "CLOSED."

c. **EKMS Account Personnel Action**:

(1) Continue to conduct all required inventories in accordance with Article 766 that may occur while undergoing the disestablishment process, and report completion of the physical inventory in accordance with Article 766.f.

(2) Ensure any Controlling Authority responsibilities, if applicable, are disestablished or transferred to another Key Management Entity.

(3) Submit MOAs to CONAUTHs of traditional keymat to request disposition authorization.

(4) Process and receipt for all in-transit material and reconcile IRST discrepancies IAW Annex AK.

(5) Submit monthly Change of Account Location (COAL) inventories as required in Article 766.b.4, and upon requests from a COR manager.

(6) Submit a Monthly Disestablishment Status Report in accordance with Article 820.

(7) As disposition instructions from NCMS and CONAUTHs are received, destroy and transfer material as directed, and report applicable transactions to the COR via x.400.

(8) When directed by the COR, submit a Final COAL inventory to the COR and print and process the IRST

(9) Print the year's transaction log.

(10) When directed by the COR, submit the Final Disestablishment Report.

(11) Upon receipt of Final Records Clearance message, ship peripherals as directed.

(12) Disposition of Records in accordance with Article 840.

d. **RESPONSIBILITIES OF IMMEDIATE SUPERIOR IN COMMAND (ISIC)**:

1. ISICs are responsible for validating the requirement to disestablish an EKMS account prior to the account being disestablished by NCMS.

2. ISICs should make every effort to verify that all COMSEC material has been properly disposed of and that the applicable documentation supporting the disposition of materials has been correctly prepared and forwarded to NCMS COR. Any discrepancies discovered by the COR during the disestablishment review must be resolved by the ISIC if the decommissioning or disestablishment occurs pending final clearance.

3. ISICs must retain; the chronological files for the account being disestablished for the current plus previous two years, the final clearance when provided by NCMS, and copies of appointment letters for the EKMS Manager and alternates for a minimum of one year following final disestablishment clearance.

4. Submit a Final Disestablishment Report, in accordance with this Chapter for accounts of commands disestablished or decommissioned prior to receipt of the final clearance message from NCMS.

815. DISPOSITION OF COMSEC MATERIAL:

a. All COMSEC material, physical and electronic, must be disposed of in accordance with the disposition instructions received from the Controlling Authority or NCMS, as applicable.

b. USMC accounts will request disposition instructions for equipment associated to the LMD/KP, NAVAIR, and MATCALS as applicable to NCMS. All other USMC owned equipment will either be transferred to another supporting EKMS account or disposed of IAW MCO 2281.1A.

c. USCG accounts will submit disposition requests for all COMSEC equipment with exception to the LMD/KP action to COGARD C4ITSC ALEXANDRIA VA//BOD-IAB// with NCMS reflected as an info addee. USCG accounts will make NCMS the action addee and COGARD C4ITSC ALEXANDRIA VA//BOD-IAB// the info addee on disposition requests for the LMD/KP.

d. If the account being disestablished is the Controlling Authority for any material, the account must submit a message to DIRNSA FT GEORGE G MEADE MD, DIR TIER1 SAN ANTONIO TX, CSLA TIER1, info NCMS WASHINGTON DC, CMIO NORFOLK VA, and all accounts validated for the material to advise all that the short title will be cancelled, production and distribution terminated and provide disposition instructions for all editions held or in-transit.

e. Unsealed keying material, maintenance manuals, operating manuals, amendments, resealed keying material and cards, printed wiring assemblies or components associated with repair (Q-kits) must be page checked prior to transfer or destruction. Page check discrepancies must be reported in accordance with Annex V.

f. Transfer, destruction, and relief from accountability reports for ALC-1, 2, and 6 material must be submitted to the COR to ensure these items are taken off-charge to the account.

820. **Monthly Disestablishment Status Messages**

a. Following submission of a message requesting disestablishment, commands will submit monthly disestablishment status messages to NCMS, info their ISIC, by the 5th working day of each month until disestablished. The message will include:

1. The total number of line items still held.

2. A statement that indicates whether disposition instructions have been requested from the applicable Controlling Authorities (for traditional keying material held) or NCMS (equipment).

3. The DTG of any pending disposition messages which a response has yet to be received for.

4. a statement certifying the account manager is working with a COR manager for any outstanding Inventory Reconciliation Status Transaction (IRST) discrepancies, the date of the most recent communications and the NCMS COR POC working with the manager. The account will not be reconciled nor should responsible personnel (the EKMS Manager, Alternates and CO) consider themselves properly relieved of responsibility in accordance with Articles 450, 455 and Chapter 8 of Navy Regulations when accounting errors exist with the units account.

830. FINAL DISESTABLISHMENT REPORT:

a. The final step in account disestablishment requires that the command send a Final Disestablishment Report to NCMS WASHINGTON DC, the respective COR, DIR TIER1 SAN ANTONIO TX **or DIR** TIER1 FORT HUACHUCA, DIRNSA, the EKMS CF, and info the administrative chain of command and keying material controlling authorities. If account holdings included modern keys (e.g., STE keying material), the following must also be included as info addressees: the CMDAUTH, if other than account's CO/OIC; and UR, if the person performing this function was attached to another command/activity.

b. Submission of this report indicates that all COMSEC material has been properly disposed of and that account records are accurate and up-to-date.

c. The ISIC must submit the Final Disestablishment Report for commands deactivated/decommissioned prior to receipt of the final clearance message.

d. The Final Disestablishment Report shall state that the COMSEC material was properly disposed of in accordance with NCMS, USCG or USMC disposition instructions, and identify the last transaction date and TN number. The report will also include the ISIC's contact information for which the EKMS-related files and records were forwarded.

e. The manager will verify and certify there are no outstanding IRST discrepancies or COMSEC material still held in the account and will provide the files and records in the following article to the ISIC.

840. DISPOSITION OF RECORDS:

a. The account will retain all EKMS-related files and records until final clearance has been received from NCMS via official message.

b. Upon receipt of the final clearance message, provide a copy of the final clearance to the ISIC, as well as the account's chronological files for the current and previous two (2) years as well as appointment letters for the EKMS manager and alternates for the same period.

c. Should a command or unit be deactivated or decommissioned prior to receipt of the final clearance message, the EKMS Manager must provide the ISIC with; the accounts chronological files for the current and previous two (2) years; appointment letters for the EKMS manager and alternates for the same period; the printed IRST associated with the last COAL generated and the current year transaction log. The EKMS Manager must also provide NCMS with the contact information for the ISIC (email/phone number and message PLA).

d. The ISIC will retain the final clearance message, chronological files, and appointment letters for a minimum of (2) years from the date time group of the final clearance message.

850. COMMAND-TO-COMMAND TRANSFER OF AN EKMS ACCOUNT:

a. When a new ISIC is involved, the losing ISIC must negotiate the transfer with the gaining ISIC and establish the date the process will be completed.

b. The losing ISIC provides the following EKMS account documentation to the new ISIC:

(1) Account validation documents.

(2) Storage/Physical Security approval documents.

AMD-9

(3) ~~EKMS Inspection~~ COR Audit documentation

c. The gaining ISIC will:

(1) Validate the account holdings.

(2) Validate storage and Physical Security requirements.

(3) Inform Controlling Authorities of the transfer as required by Article 405.c.

(4) Issue pertinent EKMS instructions to the new account.

AMD-9

(5) Review prior ~~EKMS Inspection~~ COR Audit results for the account and determine the timeframe to perform the next ~~inspection~~ audit.

(6) Send the message to NCMS and provide:

(a) Command Title/Account Number.
(b) Date transfer takes effect.
(c) ISIC'S Command Title/PLA.
(d) HCI (IF CHANGED).
(e) Statement that the account meets or will meet storage and Physical Security requirements the date the transfer takes effect.
(f) Any changes to required material.
(g) Any changes to shipping instructions.

d. The Losing EKMS Manager will:

AMD-9

(1) Inform the servicing ~~CMS A&A~~ COR Audit Team of the new command.

(2) Update Defense Courier Service (DCS) documents, i.e., if a geographical change is involved.

(3) Provide LEs with instructions/guidance from gaining ISIC.

(4) Inform the gaining ISIC of any Controlling Authority responsibilities performed by the account.

(5) Change all existing account documents to reflect the new Command/ISIC title.

(6) Ensure the Emergency Action Plan is updated in accordance with the gaining ISIC's instructions.

860. <u>Best Practices/Lessons Learned</u>:

a. As applicable, ensure all In-Transit items are received and receipted for prior to disestablishment of an account.

b. Review all MOA/LOA agreements to ensure another organization's mission is not negatively impacted.

c. If new EKMS personnel are going to be appointed to EKMS Manager positions, obtain the school quotas as early as possible.

d. As applicable, don't forget about the Controlling Authority responsibilities performed by losing accounts.

e. **For gaining ISIC's:** It is recommended that an unofficial EKMS inspection be performed using the guidance contained in EKMS-3(series) as soon as possible soon after the transfer is completed.

f. **For gaining EKMS Managers:** Soon after new LE personnel join your command, it is recommended that the EKMS Manager review the applicable portions of EKMS-3(series) with the LE personnel to provide training and guidance.

g. **For gaining EKMS Managers:** Inform the Command Security Manager of new LE personnel whose duties will require access to COMSEC material to ensure security clearance data is up-to-date, maintained and properly reflected in JPAS/JCAVS, as applicable.

CHAPTER 9 -- COMSEC INCIDENT REPORTING

FIGURES:

CHAPTER 9 - COMSEC INCIDENT REPORTING

901. INTRODUCTION TO THE NATIONAL COMSEC INCIDENT REPORTING SYSTEM (NCIRS):

a. **General**: To some degree, every item of COMSEC material is accounted for and controlled because of the role it plays in the cryptographic processes that protect or authenticate U.S. government information transmitted electronically. To counter the threat to secure communications posed by COMSEC material mishandling, losses, or thefts, the National Security Agency (NSA) established the National COMSEC Incident Reporting System (NCIRS).

b. **Purpose**: The NCIRS serves primarily to ensure that all reported incidents involving the security and integrity of COMSEC material are reported and evaluated properly so that the responsible officials can initiate action to evaluate and minimize the adverse impact to the National Security Systems (NSS). The NCIRS is comprised of organizations within the NSS community responsible for the reporting and evaluation of COMSEC incidents. The Evaluating Authority (EVALAUTH), formerly known as the Closing Action Authority (CAA) is responsible for evaluating COMSEC incidents.

905. NATIONAL SECURITY AGENCY (NSA):

To support NCIRS, NSA is responsible for operation of the NCIRS database, which provides national trend analysis reports to departments and agencies to promote COMSEC awareness and remedial action. NSA serves as the EVALAUTH for the following COMSEC incidents:

a. Cryptographic incident

b. Personnel incidents

c. Physical incidents when:

(1) NSA is the CMDAUTH or CONAUTH for the material;

(2) The CMDAUTH or CONAUTH cannot be identified;

(3) Positive Control Material (PCM)/Sealed Authenticator System (SAS) is involved. The Joint Staff evaluates PCM incidents after initial receipt at the unit level per CJCSI 3260.01.

(4) USSTRATCOM controlled codes or keying material is involved

(5) COMSEC material delivered to or for use by foreign entities

(6) Keying material used for the Global Positioning System (GPS).

(7) Suspected or known tampering; sabotage; evidence of covert penetration of packages; evidence of unauthorized or unexplained modifications to COMSEC equipment, unexplained KP zeroization or damage, evidence of unexplained modification/ damage to security containers, or vaults where COMSEC material is stored; emergency destruction and COMSEC material other than keying material (e.g., documents, algorithms, logic).

910. NAVAL COMMUNICATIONS SECURITY MATERIAL SYSTEM (NCMS):

Within the NCIRS, the NSA has established COMSEC Incident Monitoring Activities (CIMA); each service has its own CIMA activity.

a. As the DON CIMA, NCMS is responsible for:

(1) Establishment of policy and procedures to ensure that COMSEC incidents are reported promptly to the specified authorities.

(2) Entering COMSEC incidents reported into the NCIRS database.

(3) Forwarding COMSEC incidents and related reports via quoted message, SIPRNET email or other approved secure method, dependent upon the classification of the information to the CMDAUTH or CONAUTH, when not included in the COMSEC incident reported.

(4) Provide the NSA Office of Insecurities with Trend Analysis data on COMSEC incidents at a minimum of annually for the prior calendar year.

(5) Evaluating Physical Incidents involving:

a. Multiple CONAUTHs; the CIMA for the respective service of the violating unit will serve as the EVALAUTH when multiple Short Titles are involved and CONAUTHs are from different services, i.e. Army, Air Force, etc…

b. Unauthorized offer or sales of government-owned OMSEC material. NSA will be the final reviewer (EVALAUTH) upon collect and report of all related information.

915. CONTROLLING AUTHORITIES (CONAUTH)/COMMAND AUTHORITIES (CMDAUTH):

a. CONAUTH responsibilities are outlined in Annex C to this publication. With regards to COMSEC incidents, CONAUTHs will:

(1) Provide EVALAUTH for physical incidents involving Traditional COMSEC material (authenticators, code books, keying material) under their purview.

(2) Provide assessments and inform the appropriate CIMA and NSA within 10 working days following receipt of the initial report.

(3) Provide damage assessments to organizational leadership and initiate recovery actions including precautionary or emergency supersession for materials when a COMSEC incident has been assessed as "COMPROMISE".

(4) Provide a final evaluation of COMSEC incidents involving material under their purview per Annex C herein.

b. CMDAUTH responsibilities are outlined in Annex AE to this publication. With regards to COMSEC incidents, CMDAUTHs will:

(1) Receive and provide preliminary evaluations involving Modern Keying material under their purview.

(2) Solicit additional information not contained in the initial COMSEC Incident Report, when necessary to make and submit an evaluation to NSA.

(3) Initiate compromise recovery actions as discussed in Annex AE herein.

(4) Provide NSA, via the fastest, secure means available with the Key Management Identification Number (KMID) to ensure it is placed on the Compromised Key List (CKL).

920. DEPARTMENT OF THE NAVY (DON) RESOURCE MANAGERS:

a. DON Resource Managers perform and coordinate DON service planning and funding for designated COMSEC material resources. Within the DON, COMNAVIDFOR and NCMS serve as resource managers for certain paper COMSEC material and material-related items.

b. CNO is the DON resource manager for COMSEC equipment. For the purpose of distribution analysis and planning, CNO conducts appropriate consultation and coordination with NCMS and SPAWARSYSCEN ATLANTIC Charleston.

c. To fulfill the responsibilities as the DON COMSEC Incident Monitoring Activity (CIMA), NCMS//N5// **must** be included as action or information addressee on COMSEC incident reports as required by this chapter.

925. EVALUATING AUTHORITY (EVALAUTH):

An administrative senior or other designated command that reviews details of COMSEC incidents to assess the possibility a compromise has occurred. The EVALAUTH determines the need for further actions and reporting. See Article 955 for identification and responsibilities of EVALAUTH.

930. GUIDANCE ON COMSEC INCIDENT REPORTING:

a. **General**: To be effective, the NCIRS must receive prompt and clear information relating to the circumstances surrounding an incident. This information is critical to the rapid initiation of appropriate damage limitation or recovery measures by the evaluating authority.

b. **Disciplinary action**: Disciplinary action should **not** be taken against individuals for reporting a COMSEC incident unless the incident occurred as the result of willful or gross neglect by those individuals.

c. **Applicability**: The COMSEC incident reporting requirements of this chapter apply to the following:

(1) Classified and unclassified COMSEC keying material marked or designated CRYPTO (includes NSA-produced electronic key and tape key and field-generated electronic key generated from a key variable generator (e.g., KG-83/KGX-93/KP)) or STE Operational and Seed Key.

(2) Controlled Cryptographic Item (CCI) equipment.

(3) Classified COMSEC equipment.

(4) Removable media (e.g., floppy disks) containing key or other EKMS information.

(5) Malicious codes/viruses on the EKMS or KMI system.

(6) Classified COMSEC-accountable maintenance manuals, operating instructions, and publications.

d. **Unclassified COMSEC material**:

Incidents involving unclassified non-CCI equipment and related devices, unclassified publications, manuals, STE Test key, operating instructions, and unclassified key **not** marked or designated CRYPTO will be reported in accordance with Chapter 10.

e. **JCS-Positive Control material**:

Report incidents involving JCS-positive control Nuclear Command and Control (i.e., SAS (Sealed Authenticator System) two-person controlled) material in accordance with CJCSI 3260.01(series)).

f. **NATO material**:

Report incidents involving COMSEC material designated for NATO use in accordance with SDIP-293.

g. **GPS Receivers:**

(1) **UnKeyed:** When unkeyed, a lost GPS Receiver is not a COMSEC Incident however, it is reportable via SIPRNET email to:

Action: SATCOMCOMSEC@STRATNETS.STRATCOM.SMIL.MIL

Subj: REPORTABLE LOST GPS RECEIVER

The message should contain all available information (i.e. nomenclature of the GPS receiver, type, serial number etc.) and whether the device was keyed or unkeyed.

(2) **Keyed:** Report the loss of a keyed GPS receiver as follows:

Action: USSTRATCOM SATCOM COMSEC CONAUTH OFFUTT AFB NE

Info: NCMS WASHINGTON DC//N3/N5/N7//

If the CONAUTH, determines the incident warrants DIRNSA assessment/evaluation, the CONAUTH will so advise DIRNSA //I3132//.

h. **Classification and transmission**:

(1) All COMSEC incident messages will be classified a minimum of **CONFIDENTIAL** except those involving unclassified Data Encryption Standard (DES) Key which will be classified UNCLAS FOUO. Classify incident reports at higher levels according to the content of the message or letter text.

(2) Any incident report involving possible compromise of Two-Person-Controlled (TPC) material must be classified at a minimum of SECRET.

(3) Submit reports in message format via the General Service (GENSER) message system or appropriately classified, signed DMS message.

(4) The use of secure facsimile is only authorized when a message cannot be submitted. If secure fax is used, the originator of the message is responsible for ensuring proper delivery to all required agencies. Refer to Article 960 for message precedence requirements.

(5) Initial and amplifying message reports are excluded from MINIMIZE restrictions.

i. **How to use this chapter to report a COMSEC incident**:

	Article to Review:
a. Determine whether the COMSEC incident reporting requirements of this chapter apply to the COMSEC material in question. For example, incidents involving unclassified equipment (not designated CCI) or other unclassified not marked/designated as "CRYPTO" are reportable in accordance with Chapter 10.	930
b. Determine the type or category of COMSEC incident being reported (i.e., CRYPTOGRAPHIC, PERSONNEL, and/or PHYSICAL). This will help determine action and information addressees (see subparagraph (4) below).	945

c. Determine the types of COMSEC incident report 950
required. These articles also outline report precedence, 960
timeframes, format, content, and classification 965
requirements. 975

d. Determine initial and amplifying report addressees. 970
Note the type of incident category, type of COMSEC material involved, who controls it (or promulgates it) dictates report action and information addressees.

e. Determine whether the incident to be reported 935
requires accounting actions.

f. What is a final letter report? When might one be 975
required of your command, and who may require it?

g. Finally, use the COMSEC Incident Report Format/Content Checklist in Figure 9-1 at the end of this chapter. It will help you verify that you have supplied all of the information required for a swift evaluation. An example final letter report is shown in Figure 9-2.

935. SF-153 RELIEF FROMACCOUNTABILITY AND POSSESSION REPORTS RELATED TO COMSEC INCIDENTS:

A Relief from Accountability or Possession Report is required when COMSEC material is unable to be accounted for (lost) or found and there exists no accounting report (Destruction, Relief from Accountability or Transfer SF-153) or the material is not currently reflected on the unit’s Accountable Item Summary (AIS), as applicable.

a. A SF-153 **Relief from Accountability Report** must be prepared whenever a whole edition, complete short title, or separately accountable end item of COMSEC accountable material is missing **and** no documentation exists which indicates that the item was either transferred or destroyed. Failure to generate and submit this report when required will result in the missing item continuing to be reflected as In-Stock to the account in Tier-1 or reflected on the units AIS.

A Relief from Accountability Report must also be submitted to the COR when missiles with embedded COMSEC are fired per Annex AB. Do not submit a Relief from Accountability report to the COR for ALC-4 or ALC-7 material; retain it locally in the accounts chronological file.

NOTE: The loss of individual segments, pages of manuals or equipment items accounted for only as components of an end item must be reported in accordance with Annex U.

b. A SF-153 **Possession Report** must be generated and submitted to the COR whenever a whole edition, complete short title, or separately accountable end item of COMSEC accountable material comes into the possession of an account and either of the following is true:

(1) There is no documentation that the found material was ever held by, generated by, or "In Stock" to the account, **OR**

(2) The physical material was previously held by the account but was properly documented as transferred or destroyed in LCMS.

(3) Do **not** submit an SF-153 Possession Report whenever a whole edition, complete short title, or separately accountable end item of COMSEC accountable material is found that was documented as destroyed and reported to NCMS as destroyed, instead follow these instructions:

(a) Report the finding of the material as a PHYSICAL incident in accordance with Article 945.

(b) If the material is authorized for destruction, destroy it and document the **actual** destruction locally. Indicate in the incident report the found material was destroyed.

(c) If the found material is not authorized for destruction (e.g., found material is equipment or future key previously reported as "prematurely" destroyed), request disposition instructions in the incident report.

940. REPORT SUBMISSION GUIDANCE:

a. Any unit detecting a COMSEC incident will promptly report it in accordance with this chapter. Reporting units do not have to be the unit that caused the incident. For example, incidents involving the use of unapproved transportation methods to ship COMSEC material are most often reported by the recipients of the shipment as opposed to the originators.

b. When an incident occurs with an external LE, the LE command or command owning the six-digit account will report the incident per the local COMSEC instruction or LOA/MOU promulgated by the supporting six-digit account command. Locally prepared COMSEC instructions and/or LOAs/MOUs must clearly outline who is responsible for the reporting and how they are to be reported.

NOTE: Annex L contains a sample Letter of Agreement with the minimum requirements to be addressed.

AMD-9

c. The servicing ~~A&A~~ COR Audit Team must be included as an information addressee on all initial and amplifying reports.

945. CATEGORIES AND EXAMPLES OF COMSEC INCIDENTS:

a. **General**: The incident listing herein is not all inclusive. Additional reportable incidents unique to a given cryptosystem or device will be listed in the cryptographic operating instruction (KAO) and cryptographic maintenance manual (KAM) or Operational Security Doctrine (OSD) for the cryptosystem or device. Accordingly, each command must ensure these documents are reviewed during COMSEC incident/insecurity familiarization training. Incidents uniquely related to DTDs, STEs (and related cards), SKLs and TALON cards can be found in Annexes; Z, AC, AD, and AF.

b. COMSEC incidents are divided into **three categories**:

(1) Cryptographic

(2) Personnel

(3) Physical

c. **Examples of Cryptographic Incidents**:

(1) Use of COMSEC keying material that is compromised, superseded, defective, previously used (and not authorized for reuse), or incorrect application of keying material; such as:

(a) Use of keying material produced without NSA authorization (e.g., homemade maintenance, use of keying material on compact disks (CDs) duplicated without authorization from the CONAUTH).

NOTE: NSA authorization to generate key in the field is implicitly stated in the security doctrine or operating instructions for devices which possess such capability.

(b) Use, without NSA authorization, of any keying material for other than its intended purpose.

(c) Unauthorized extension of a cryptoperiod.

(d) Use or attempted use of a Key Generator/Key processor (e.g., KG-83, KGX-93, KOK-23, KP, AKP) beyond its mandatory recertification date without prior approval.

(e) Use of modern key with the same Keying Material Identifier (KMID) loaded in more than one End Cryptographic Unit (ECU).

(f) Premature use (defined as an on-the-air attempt to establish communications/transmit data) or out-of-sequence use of keying material without the consent of the CONAUTH.

(2) Use of COMSEC equipment having defective cryptographic logic circuitry, <u>or</u> use of an unapproved operating procedure; such as:

(a) A connection between the LMD and a TOP SECRET system/device other than the KP.

(b) Plain text transmission resulting from a COMSEC equipment failure or malfunction.

(c) Any transmission during a failure, or after an uncorrected failure that may cause improper operation of COMSEC equipment.

(d) Operational use of equipment without completion of required alarm check test or after failure of required alarm check test.

(3) Use of any COMSEC equipment or device that has <u>not</u> been approved by NSA.

(4) Detection of malicious codes (VIRUSES) on the EKMS system (LMD/KP).

(5) Operational use of an In-Line Network Encryptor (INE) which is not compliant with a mandatory software upgrade by the compliance date without a waiver from NCF or DIRNSA.

(6) Use of a Key Encryption Key (KEK) classified lower

than the Traffic Encryption Key (TEK) passed during OTAD/OTAT operations, except during a COMSEC emergency.

(7) Failure to perform KP changeover as described in Article 238, or more frequently as required. Incident reports submitted to report failure to perform a KP changeover will reflect NAVREINIT2 as the Short Title in Para (2) of the COMSEC Incident report. There is no edition for these items.

(8) Unauthorized extension of the Storage Key Encryption Key (SKEK) or Local Key Encryption Key/Host Data Protection Key (LKEK/HDPK) cryptoperiod for the DTD or SKL respectively, as applicable. This includes failure to maintain documentation to verify annual reinitialization requirements set forth in Annexes Z, AF and the applicable Operational Security Doctrine for the device(s).

NOTE: The cryptographic incident noted in 945.c.9 would occur when a DTD and/or SKL storing key is not initialized annually, as required. This is not applicable to devices NOT initialized and/or storing key.

(9) Use of an algorithm or mode decertified by NSA, as well as use of keying material developed for a decertified algorithm beyond the cease key date without approval per CJCSI 6510.02.

(10) Any other occurrence that may jeopardize the crypto security of a COMSEC system.

d. **Examples of Personnel Incidents**:

(1) Known or suspected defection and/or espionage.

(2) Capture by an enemy of persons who have detailed knowledge of cryptographic logic or access to keying material.

(3) Unauthorized disclosure or attempts by unauthorized personnel to affect disclosure related to COMSEC material, Personal Identification Numbers (PINs) or passwords that could enable unauthorized secure use of a wired/wireless device

(4) Deliberate falsification of COMSEC records.

e. **Examples of Physical Incidents**:

(1) The physical loss of COMSEC material; includes whole

editions as well as a classified portion thereof (e.g., a classified page from a maintenance manual, keytape segment).

NOTE: If a record of destruction, transfer or relief from accountability report is required but is not available, the material must be considered lost.

(2) The loss or compromise of any of the following:

(a) KP CIKS and non-zeroized KP KSDs-64As (e.g., REINIT 1 AND NAVREINIT 2).

(b) KP keys (EKMS FIREFLY and EKMS MSK).

(c) Removable media (e.g., floppy disks) containing key or other EKMS information.

(d) KP PINS.

(e) CIK or Card. When the CIK/Card can be identified with a particular secure voice or data terminal and it was not zeroized from the terminal.

(3) Failure to adequately protect or erase a CIK or card that is associated with a lost secure voice or data terminal.

(4) Failure to review audit trail data and maintain an audit review log for equipment with audit capability (e.g., DTD, SKL, TKL, etc…) which **have been/are initialized, storing key or issued to a LE since the previous audit trail review was conducted**, per the requirements outlined in the specific cryptosystem doctrine.(See Annex Z paragraph 17.c (note 3) and Annex AF paragraph 9.b (note 3) for exceptions to the audit review policy.

(5) Unauthorized access to COMSEC material by persons inappropriately cleared. **This includes non-establishment of SCI eligibility in JPAS and SCI indoctrination for EKMS Managers, Alternates and LE Issuing when validated for and/or holding such material.**

(6) COMSEC material discovered outside of required accountability or physical control, for example:

(a) Material reflected on a destruction report as having been destroyed and witnessed, but found not to have been destroyed.

(b) Material left unsecured and unattended where unauthorized persons could have had access (e.g., leaving a LMD/KP terminal unattended after an Administrator or Operator has logged on and the KP PIN has been entered).

(c) Missing or non-use of required LCI documentation for material issued to user personnel. This includes instances where documents not meeting the criteria of Article 712 are substituted for LCI documents.

(7) Failure to maintain required TPI for TOP SECRET keying material, except as indicated in Article 510.f or where a waiver has been granted. For example:

(a) Single person access to unencrypted TOP SECRET keying material marked or designated CRYPTO, except when authorized in an emergency, (including FDs containing unencrypted TOP SECRET keying material).

(b) Single person access to the KP during TPI mode operations (i.e., generating unencrypted TOP SECRET keying material).

(8) COMSEC material improperly packaged or shipped.

(9) Receipt of classified equipment, and keying material marked or designated CRYPTO with a damaged inner wrapper.

(10) Destruction of COMSEC material by other than authorized means.

(11) COMSEC material not completely destroyed and left unattended. This includes failure to properly demilitarize equipment, when authorized.

(12) Actual or attempted unauthorized maintenance including maintenance by unqualified personnel or the use of a maintenance procedure that deviates from established standards.

(13) Tampering with, or penetration of, a cryptosystem; for example:

(a) COMSEC material received in protective packaging (e.g., key tape canisters) which shows evidence of tampering.

(b) Unexplained (undocumented) removal of keying material from its protective technology.

(c) Known or suspected tampering with **or** unauthorized modification of COMSEC equipment.

(d) Discovery of a clandestine electronic surveillance or recording device in or near a COMSEC facility.

(e) Activation of the anti-tamper mechanism on, or unexplained zeroization of, COMSEC equipment (e.g., KP) when other indications of unauthorized access or penetration are present.

NOTES: 1. Hold information concerning tampering with COMSEC equipment, penetration of protective technologies, or clandestine devices on a strict need-to-know basis. Immediately and simultaneously report such to NSA, the CONAUTHs, and other information addressees in Article 965.

2. When tampering or penetration is known or suspected, wrap and seal the material along with all protective technologies and place the package in the most secure, limited-access storage available. The material must not be used or otherwise disturbed until further instructions are received from NSA.

3. Where a clandestine surveillance or a recording device is suspected, do not discuss it in the area of the device. Take no action that would alert the COMSEC exploiter, except that provided in instructions from the applicable counterintelligence organization or NSA. Take no action that would jeopardize potential evidence.

(14) Unauthorized reproduction, photographing or copying of COMSEC material (including cloning devices storing key without proper documentation).

(15) Inadvertent destruction or destruction of COMSEC material without the authorization of the Controlling Authority or Service Authority, as applicable.

(16) Late destruction of **any** COMSEC material, including key in a fill device, and unclassified material (i.e., destruction not completed within the timeframes in this manual) except where a waiver has been granted. For superseded material received in a Reserve on Board (ROB) shipment from DCS see Article 620.d and if destroyed within 12 hours of receipt, do

not report this as a COMSEC incident.

(17) Emergency Destruction of COMSEC material.

(18) Any other incident that may jeopardize the physical security of COMSEC material.

950. TYPES OF COMSEC INCIDENT REPORTS & SUBMISSION REQUIREMENTS:

a. There are three types of incident reports:

(1) Initial
(2) Amplifying
(3) Final

1. **Initial Report**:

Submit for each COMSEC Incident. If all facts regarding the incident are included in the initial report, it may be accepted as a final report by the appropriate Evaluating Authority (EVALAUTH) identified in Article 955.

2. **Amplifying Report**:

Submit whenever significant new information is discovered or is requested by the evaluating authority. An amplifying may also serve as a final report, if so accepted by the appropriate EVALAUTH.

3. **Final Report**:

Submit only if specifically requested by the appropriate EVALAUTH identified in Article 955.

NOTE: See Article 975 for final report format, content, and submission requirements.

955. DON EVALUATING AUTHORITIES AND RESPONSIBILITIES:

a. **Identification of EVALAUTHs**:

COMMAND PREPARING REPORT:	**EVALAUTH:**
Coast Guard	COGARD C4ITSC ALEXANDRIA VA//BOD-IAB//
Marine Corps	CMC C FOUR CY WASHINGTON DC//
Military Sealift	COMSC WASHINGTON DC//N62M//
Navy Fleet/shore activities administratively subordinate to a COMFLT	COMUSFLTFORCOM NORFOLK VA//N023EKMS// **OR** COMUSNAVEUR COMUSNAVAF NAPLES IT//N6// **OR** COMPACFLT PEARL HARBOR HI//N633//
Navy shore activity not administratively Subordinate to a COMFLT or COMSC	NCMS WASHINGTON DC//N5//
Naval Reserve force Units and activities	COMNAVRESFOR NORFOLK VA//01D//

NOTE: If required by the EVALAUTH, the final report will be submitted within 30 days from the initial report or the last amplifying report. The final report will include a summary of results of all inquiries and investigations, and it must identify corrective measures taken or planned to minimize the possibility of recurrence. Corrective measures will be provided to the CONAUTH by separate message or be included in an Amplifying report.

b. **EVALAUTH Responsibilities**:

(1) The EVALAUTH determines the need for further reporting and has the authority to request a final report for COMSEC incidents evaluated as "**COMPROMISE**"." Each EVALAUTH message or letter request for a final letter report must be addressed as follows:

FROM: EVALAUTH
ACTION: Violating Command
INFO: Administrative Chain Of Command
OR
Operational Senior (as appropriate)
NCMS WASHINGTON DC//N5//

AMD-9

Servicing ~~A&A~~ COR Audit Team

Subject: REQUEST FOR FINAL LETTER REPORT

(2) EVALAUTHs must formally "close-out" only those cases for which a final letter report has been requested.

(a) After receiving the final letter report, the EVALAUTH will affect case closure by issuing a Closing Action Letter or Message to the violating command.

(b) The administrative chain of command or Operational Senior of the violating command and NCMS//N5// must be included as copy to/information addressees.

(c) An example Closing Action Letter is provided in Figure 9-3.

c. **NCMS Responsibilities**:

(1) Whenever a COMSEC incident is reported, NCMS as the DON CIMA, establishes an incident case file for the violating command. This case file facilitates tracking of all reports associated with the incident.

(2) NCMS is also responsible for closing-out incident cases following submission of all required reports.

(a) Incident cases pending a final report will remain open until NCMS receives the EVALAUTH Closing Action Letter or Message.

(b) NCMS will close all other incident cases 30 days after receipt of the initial and/or amplifying report.

960. PRECEDENCE AND TIMEFRAMES FOR SUBMITTING INITIAL REPORTS:

Initial incident reports must be reported by message in accordance with the following precedence and timeframes:

a. Submit an **IMMEDIATE** precedence message within **24 hours** after discovery if the incident involves:

(1) Effective key or key scheduled to become effective within 15 calendar days.

(2) Incidents involving defection, espionage, hostile

cognizant agent activity, theft, tampering, clandestine exploitation, sabotage, , or unauthorized copying, photographing or reproduction.

(3) Incidents involving Nuclear Command and Control (NC2) material.

NOTE: Following submission of an IMMEDIATE precedence incident report, the reporting command must ensure that an individual familiar with the details of the incident report is available to rapidly respond to possible questions from the evaluating authority.

b. Submit a **PRIORITY** precedence message within **48 hours** after discovery if the incident involves: Future key scheduled to become effective in more than 15 calendar days, Superseded key, Reserve on board (ROB) key, or Contingency key.

c. Submit a **ROUTINE** precedence message within **72 hours** after discovery if the incident involves any incident **not** covered above.

NOTE: Neither a local command inquiry nor investigation in progress by an external agency such as NCIS excuses commands from complying with the incident reporting timeframes set forth in this manual. When it is believed that reporting an incident through normal naval message channels might compromise an investigation in progress, the violating command must contact DIRNSA (I3132) or NCMS (N5) by other secure means to provide information concerning the incident.

d. Report incidents involving codebooks per the timeframe stipulated by the CONAUTH on codebook cover page.

965. ADDRESSEES FOR COMSEC INCIDENT REPORTS:

a. This matrix in this article provides the **minimum** addresses required when a COMSEC incident report is submitted.

b. Where two-holder, point-to-point material is involved, the organization or unit that established the circuit will normally serve as CONAUTH.

MINIMUM ADDRESSEES REQUIRED TO BE ON COMSEC INCIDENT REPORTS

Organization	Action/ Info	Remarks
DIRNSA FT GEORGE MEADE MD //I3132//	A/I	Action on; - all CRYPTOGRAPHIC and PERSONNEL incidents - Physical incidents involving tampering, sabotage, covert penetration. - Physical incidents where there are multiple CAs and they are not all DON. (**Info on others**)
NCMS WASHINGTON DC//N5//	A/I	Action on; - Physical incidents when a DON CA is the violator - Physical incidents with more than one DON CA and all are DON. (**Info on all others**)
COMNAVIDFOR SUFFOLK VA	I	Info addee on all reported COMSEC incidents
CNO WASHINGTON DC	I	On all incidents involving the loss of classified material **(The initial COMSEC incident report satisfies the mandatory Preliminary Inquiry (PI) requirement in SECNAV M5510.36 (12-8) when the CNO N09N2, DIRNSA and the local NCIS field office are included in the report.**
CMC C FOUR CY WASHINGTON DC	I	All USMC units will ensure CMC Washington is an info addee on all incident reports.
COMSC WASHINGTON DC	I	For incidents involving keying material controlled by COMSC, address as an action addee. For other incidents, all MSC activities will ensure COMSC Washington is an

		info addee on all related message.
COMNAVRESFOR NORFOLK VA	I	All reserve force units and activities will include as an info addee.
DIRNAVCRIMINVSERV WASHINGTON DC	I	On all incidents involving the loss of classified material(**The initial COMSEC incident report satisfies the mandatory Preliminary Inquiry (PI) requirement in SECNAV M5510.36 (12-8) when the CNO N09N2, DIRNSA and the local NCIS field office are included in the report.**
The accounts nearest NCIS Field Office (afloat units with a NCIS Resident agent aboard) must include the NCISRA nearest their homeport)	I	On all incidents involving the loss of classified material (**The initial COMSEC incident report satisfies the mandatory Preliminary Inquiry (PI) requirement in SECNAV M5510.36 (12-8) when the CNO N09N2, DIRNSA and the local NCIS field office are included in the report.**
CONTROLLING AUTHORITY	A	When keying material is involved or for physical incidents involving CCI loaded with key managed by the respective CA.
COMPACFLT PEARL HARBOR (CPF) //N633//or COMUSFLTFORCOM NORFOLK VA (USFF)	A/I	Action for - incidents involving material controlled by CPF or USFF, as applicable. **For all other incidents, PACFLT and LANTFLT surface ships will include either CPF or USFF as an info addee on all incident reports.**
COGARD C4ITSC ALEXANDRIA VA//BOD-IAB//	A/I	If COGARD C4ITSC is the CA and the incident involves keying material send as action. For other incidents, USCG units will include COGARD C4ITSC as an

		info addee.
HQ USPACOM //J63//	A/I	Action for incidents involving HQ USPACOM controlled material. For incidents not involving PACOM controlled material, theater policy requires all PACOM units include HQ USPACOM an info addee.
The units Immediate Superior in Command (ISIC)	I	If keying material is involved and the ISIC is the CA, address it "Action" to the ISIC, info the other addees.
The units Operational Chain of Command	I	
Evaluating Authority (EVALAUTH)	I	**CAAs:** USCG: C4ITSC; USMC: CMC; MSC: COMSC; USN (FLEET): CPF/USFF; USN (SHORE) NCMS (N5)
Units servicing COR Audit Team	I	

(1) **CLASSIFIED COMSEC MATERIAL-RELATED PUBLICATIONS AND MANUALS PRODUCED BY NCMS**

Handle in accordance with SECNAV M5510.36 (series) and request replacement (if required) in accordance with Chapter 9 of this manual.

(2) **UNCLASSIFIED COMSEC AND COMSEC-RELATED MATERIAL**:

Report and request replacement in accordance with Chapter 10.

c. If an incident involves nuclear command and control (NC2) COMSEC material other than JCS-positive control material, address the report for action to DIRNSA FT GEORGE G MEADE MD//I2N//.

d. If an incident involves COMSEC material provided by the U.S. to allied governments, include DIRNSA FT GEORGE G MEADE MD//DP2// as an information addressee.

e. If an incident involves actual or possible penetration of protective technologies, address the report for action to DIRNSA FT GEORGE G MEADE MD//I2324//.

970. **FORMAT AND CONTENT OF INITIAL AND AMPLIFYING REPORTS**:

a. **General**:

(1) Format and content requirements are outlined below. Each of the paragraphs indicated must be addressed in all initial reports.

(2) Where the reporting requirements of a paragraph are not applicable to the incident being reported, the corresponding paragraph in the report must reflect the notation "N/A" for not applicable.

(3) Where subsequent reports (e.g., amplifying) would merely duplicate information previously reported, the information need not be repeated. Instead, reference will be made to the previous report, which contains the information.

b. **Subject of Report**: The subject of each report will be:

INITIAL REPORT OF COMSEC INCIDENT

OR

AMPLIFYING REPORT OF COMSEC INCIDENT

OR

FINAL REPORT OF COMSEC INCIDENT, as applicable

c. **References**: As applicable, the report must include references to:

(1) Identification of the paragraph number of the operating or maintenance instruction, or this manual in which the reported insecurity is listed.

(2) Previously forwarded reports relating to the incident (e.g., message date-time-group, letter serial number).

d. **Body/Text of Report**: The following information must be provided in the order presented here:

(1) **PARAGRAPH 1**: Identify the EKMS account number of the violating command or activity. If the actual violator is a LE of the EKMS account identified, state so here.

(2) **PARAGRAPH 2**: Identify the material involved as follows:

(a) **Documents, hard-copy keying material, and electronic key converted from keytape**: Include the full short title and edition; accounting number; specific segments, tables, pages, if not a complete edition or document; the classification, and the CONAUTH of each short title listed.

(b) **Field-generated key**: List the short title, key designator, tag, or other identifier; circuit designator; type of crypto equipment used to secure the circuit; and type of key generator.

(c) **Equipment** (including CCI): Include the nomenclature or system designator; modification number(s) if applicable; serial number of AL 1 equipment (all other by quantity); and associated or host equipment. If the equipment was keyed, also identify the information previously identified for keying material.

(3) **PARAGRAPH 3**: Identify the personnel involved. Provide duty position and level of security clearance. For personnel incidents **only**, also provide name and rank/grade.

(4) **PARAGRAPH 4**: Describe the circumstances surrounding the incident. Give a chronological account of the events, which led to the discovery of the incident and, when known, sufficient details to give a clear picture of how the incident occurred. If the reason for the incident is not known, describe the events that led to the discovery of the incident.

(5) **PARAGRAPH 5**: Provide the information requested below for each of the incidents that follow:

(a) **CRYPTOGRAPHIC INCIDENTS**:

1. INCORRECT USE OF COMSEC KEYING MATERIAL, COMSEC AIDS

OR

USE OF AN UNAPPROVED OPERATING PROCEDURE:

OR

PREMATURE USE OR USE OF SUPERSEDED/EXPIRED KEYING MATERIAL

--- Describe the communications activity (e.g., on-line/off-line, duplex/half-duplex/full-duplex, point-to-point/netted operations) and the operating mode of the COMSEC equipment (e.g., clock start, message indicator).

--- Estimate amount and type of traffic involved.

--- Estimate length of time the key or aid was used.

--- Provide the DTG of the Controlling Authority status message (Only required when Traditional Key is involved)

2. USE OF MALFUNCTIONING COMSEC EQUIPMENT:

--- Describe symptoms of the COMSEC equipment malfunction and how the malfunctioning product was used.

--- Estimated likelihood that the Malfunction was deliberately induced. If so, also see Item (3) of this category.

3. UNAUTHORIZED MODIFICATION OR MAINTENANCE OF COMSEC EQUIPMENT:

--- Describe the modification or device, installation, symptoms, host equipment involved, and protective technology, if applicable.

--- Estimate how long the item may have been in place.

--- Estimate the amount and type of traffic involved.

--- Identify the counterintelligence organization notified, if applicable. If so, include POC and phone number of organization notified.

(b) **PERSONNEL INCIDENTS**:

KNOWN OR SUSPECTED DEFECTION, ESPIONAGE, ATTEMPTED RECRUITMENT, UNAUTHORIZED ABSENCE, SABOTAGE, CAPTURE, HOSTILE COGNIZANT AGENCY ACTIVITY, OR TREASON:

--- Describe the individual's extent of Knowledge of COMSEC and crypto principles and protective technologies.

--- List the cryptosystems to which the Individual had recent access and Whether the access included keying material.

--- Identify the counterintelligence Organization notified (e.g., NCIS for DON accounts). Provide a point of contact and telephone number at the counterintelligence organization.

NOTE: Incidents related to unauthorized absence are to be reported only when there is missing material or reason to suspect espionage/defection.

(c) **PHYSICAL INCIDENTS**:

1. UNAUTHORIZED ACCESS TO COMSEC MATERIAL:

--- Estimate how long unauthorized personnel had access to the material.

--- State whether espionage is suspected. If so, see items under personnel incidents above.

2. LOSS OF COMSEC MATERIAL:

--- Describe the circumstances of last sighting; provide any available information concerning the cause of disappearance.

--- Describe the actions taken to locate the material.

--- Estimate the possibility that material may have been removed by authorized or unauthorized persons.

--- Consult Article 935

--- Describe the methods of disposal of classified and unclassified waste and the possibility of loss by those methods.

3. COMSEC MATERIAL DISCOVERED OUTSIDE OF REQUIRED COMSEC CONTROL OR ACCOUNTABILITY **OR** LOSS OF TPI:

--- Describe the action that caused accountability or physical control to be restored.

--- Estimate likelihood of unauthorized access.

--- Estimate the length of time the material was unsecured.

4. RECEIPT OF CLASSIFIED EQUIPMENT, CCI EQUIPMENT, OR KEYING MATERIAL MARKED OR DESIGNATED CRYPTO WITH A DAMAGED INNER WRAPPER:

--- Give a complete description of the damage.

--- If damage occurred in-transit, identify The method of shipment. Include the package number and point of origin.

--- If the damage occurred in storage, describe how the material was stored.

--- Estimate the likelihood of unauthorized access or viewing.

--- Ensure all packaging containers, wrappers, etc., are retained until disposition instructions are received.

5. KNOWN OR SUSPECTED TAMPERING WITH COMSEC EQUIPMENT **OR** PENETRATION OF PROTECTIVE TECHNOLOGY:

--- Describe the evidence of tampering or penetration.

--- If the suspected tampering or penetration occurred in-transit, identify the method of shipment.

--- Include the package number and point of origin. Retain all packaging material until disposition instructions are received.

--- If the suspected tampering or penetration occurred in storage, describe how the material was stored.

--- Identify the counterintelligence Organization notified (e.g., NCIS for DON accounts). Provide a point of contact and telephone number at the counterintelligence organization.

--- Identify the date or serial number stamped on the protective technology, as applicable.

6. UNAUTHORIZED PHOTOGRAPHY, REPRODUCTION OR COPYING OF KEY (CLONING DEVICES):

--- Identify the material or equipment that was reproduced or photographed.

--- Provide the reason for the reproduction and describe how the material was controlled.

--- Specify detail contained in the photographs of equipment internals.

--- State whether espionage is suspected. If so, also see items under the Personnel Incident Category.

--- If the incident is evaluated as "COMPROMISE" or "COMPROMISE CANNOT BE RULED OUT," forward a copy of each photograph or reproduction to NSA //I3132//.

7. AIRCRAFT CRASH:

NOTE: See Annex AB for mandatory documentation and reporting requirements for missile firings.

--- Identify the location of the crash (including coordinates), and specify whether the crash occurred in friendly or hostile territory. If the aircraft crashed at sea, also see Item (8) below.

--- State whether the aircraft remained largely intact or if wreckage was scattered over a large area. Estimate the size of the area.

--- State whether the area was secured. If so, indicate how soon after the crash and by whom.

--- State whether recovery efforts for COMSEC material was made or is anticipated.

--- Consult Article 935 of this manual to determine whether a SF-153 Relief from Accountability Report must be submitted.

8. MATERIAL LOST AT SEA:

--- Provide the coordinates (when available) or the approximate distance and direction from shore.

--- Estimate the depth of the water.

--- Estimate whether material was in weighted containers or was observed to sink.

--- Estimate the sea state, tidal tendency, and the most probable landfall.

--- State whether U.S. salvage efforts were made or are anticipated.

--- State whether foreign vessels were observed in the immediate area and their registry, if known.

--- Estimate the possibility of successful salvage operations by unfriendly nations.

9. SPACE VEHICLE MISHAP:

--- Provide the launch area and time.

--- State whether the space vehicle was destroyed or lost in space.

--- State whether the keying material involved was unique to the operation or is common to other operations.

--- Estimate the probable impact point on the surface of the earth, if applicable.
If the impact point was on land, also see Item (c) (7); if the impact point was at sea, see Item (c)(8).

10. MISSING MOBILE UNIT (e.g., land vehicle, aircraft, or ship):

--- Identify the scheduled or probable route, probable or confirmed position, and date and time of last confirmed position, if available.

--- Estimate possibility of missing unit encountering hostile forces.

--- State whether recovery efforts for COMSEC material was made or is anticipated.

10. INADVERTENT or LATE DESTRUCTION:

--- Identify the CONAUTH of the material.

--- Provide the DTG of the most recent CONAUTH status message or URL to the Site used by the CONAUTH.

--- State whether resupply is required (for inadvertent destruction of physical material; reflect N/A for Late Destruction).

(6) **PARAGRAPH 6**: State whether an investigation has been initiated, and if so, identify the type of investigation initiated (e.g., local command inquiry, NCIS, JAG).

(7) **PARAGRAPH 7**: Indicate whether an SF-153 Relief from Accountability or Possession Report will be forwarded, and if so, identify transaction number, if known.

(8) **PARAGRAPH 8**: Include the name and telephone number of an individual who is prepared to respond to questions from the evaluating authority.

(9) **PARAGRAPH 9**: Additional data

AMD-9

~~a. Date of last CMS A&A visit:~~
a~~b~~. Date of last ~~ISIC inspection~~COR Audit:
b~~c~~. Date of last semi-annual self-assessment:

975. FINAL REPORT FORMAT, CONTENT, AND SUBMISSION REQUIREMENTS:

a. **Final Report**:

(1) The final report, which may be submitted via official naval letter or message is the most comprehensive report of an incident. Final reports are required only when directed by the applicable EVALAUTH and are not authorized for transmission via naval message when MINIMIZE is imposed.

(2) The final report must be submitted to the EVALAUTH via the administrative chain of command. The following report distribution requirements also apply, as applicable:

(a) Operating forces operationally subordinate to a COMFLT but administratively subordinate to another COMFLT will submit reports to the Administrative Senior with a copy to the Operational Senior.

(b) Shore commands not administratively subordinate to a COMFLT, but which support a COMFLT, will provide a copy to that COMFLT.

(c) If NCMS is the EVALAUTH and the reporting command has imposed or is recommending disciplinary action, the final report must be forwarded via the reporting unit's next senior command with court martial jurisdiction over the incident to ensure proper legal review.

(d) Final reports must be submitted within 30 days of the initial report of the incident. EVALAUTHs will ensure that the final report is submitted within the prescribed timeframes.

(f) The final report format shown at the end of this chapter should be used whenever possible and may be submitted via naval message or official command letter head. The final report must include a comprehensive and complete report of the investigation conducted into the incident, and must state action taken by the command to prevent recurrence of the same type of incident.

980. ASSESSING COMPROMISE PROBABILITY:

a. COMSEC incidents are evaluated using one of these terms:

(1) **COMPROMISE**: A judgment, based on the preponderance of the evidence, that a disclosure of information to unauthorized persons, or a violation of the security policy for a system in which unauthorized, intentional or unintentional disclosure, modification, destruction, or loss of an object has occurred.

(2) **NO COMPROMISE**: A judgment, based on the preponderance of the evidence, that a disclosure of information to unauthorized persons, or a violation of the security policy for a system in which unauthorized, intentional or unintentional disclosure; modification; destruction; or loss of an object has not occurred.

b. Compromise probability assessment is often a subjective process, even for experienced evaluators who possess all pertinent facts concerning a COMSEC incident. To assist your command in assessing compromise probability, the following guidance is provided for the most commonly encountered or reported incidents:

(1) Lost keying material, including keying material believed to have been destroyed without documentation, and material that is temporarily out of control (i.e. believed lost but later recovered under circumstances where continuous secure handling cannot be assured or was found in an unauthorized location): Assess as COMPROMISE.

(2) Unauthorized access: If the person had the capability and opportunity to gain detailed knowledge of, or to alter information or material: Assess as COMPROMISE. If the person was under escort or under the observation of a person authorized access, or if physical controls were sufficient to prevent the person from obtaining detailed knowledge of information or material, or from altering it: Assess as NO COMPROMISE.

(3) Unauthorized absence of personnel who have access to keying material: Assess as NO COMPROMISE, unless there is evidence of theft, loss of keying material, or defection.

NOTE: Whenever a person having access to keying material is reported as UA, all material he/she could have accessed must be inventoried. If there is evidence of theft or loss of keying material, or defection of personnel, the material must be considered COMPROMISED.

c. Also see NAG-16(series) for guidance on assessing incidents involving field-generated electronic key.

985. REPORTING COMSEC INCIDENTS DURING TACTICAL DEPLOYMENTS AND DURING ACTUAL HOSTILITIES:

a. During time-sensitive tactical deployments, abbreviated reports may be submitted for incidents involving keying material where espionage is not suspected.

b. Such reports must answer the questions: who, what, where, when, and how. This type of report must be submitted promptly to the addressees in Article 965 and must provide sufficient details to enable the evaluating authority to assess whether a compromise has occurred.

c. During actual hostilities, loss of keying material must be immediately reported to each Controlling Authority or Command Authority by the most expeditious means available so that supersession or recovery actions can be taken.

d. It is recognized that there will be times when immediate reporting to activities other than the Controlling Authority serves no purpose. When keying material that is scheduled for supersession within 48 hours is lost and espionage is <u>not</u> suspected, an incident report is <u>not</u> required.

INITIAL AND AMPLIFYING COMSEC INCIDENT REPORT FORMAT AND CONTENT CHECKLIST

Subject __________

References __________

Paragraph 1: EKMS account number __________

Paragraph 2: Material involved __________

Paragraph 3: Personnel involved __________

Paragraph 4: Circumstances of incident __________

Paragraph 5: Additional information on incident required by: Article 970 d.(6):

Incorrect use of COMSEC keying material or use of an unapproved operating procedure. (a)(1)

Use of malfunctioning COMSEC equipment. (a)(2)

Unauthorized modification or maintenance of COMSEC equipment. (a)(3)

Known or suspected defection, espionage, attempted, recruitment, treason, sabotage, or capture. (b)

Unauthorized access to COMSEC material. (c)(1)

Loss of COMSEC material. (c)(2)

COMSEC material discovered outside of required control or accountability. (c)(3)

Loss of TPI. (c)(3)

Receipt of classified equipment, CCI equipment, or keying material marked or designated CRYPTO with a damaged inner wrapper. (c)(4)

Known or suspected tampering with COMSEC equipment or penetration of protective technology. (c)(5)

FIGURE 9-1

Unauthorized photography or reproduction. (c)(6)

Paragraph 5: Additional information on incident required by:
(Con't) Article 970 d.(6):

Aircraft crash. (c)(7)

Material lost at sea. (c)(8)

Space vehicle mishap. (c)(9)

Missing mobile unit. (c)(10)

Paragraph 6: Whether investigation conducted. ___________

Paragraph 7: Whether SF-153 Relief from Accountability or Possession Accounting Report will be submitted. ___________

Paragraph 8: Point of contact and phone number. ___________

Paragraph 9: Additional data.

a. Date of last COR Audit: ___________
b. Date of last semi-annual self-assessment: ___________

FIGURE 9-1-2

EXAMPLE INITIAL REPORT OF A COMSEC INCIDENT

(CLASSIFIED FOR INFORMATION PURPOSES ONLY)

```
O 301929Z SEP 09
FROM:  USS SHELLBACK
TO:    CONAUTH
INFO:  DIRNSA FT GEORGE G MEADE MD//I3132// (OMIT IF DIRNSA IS THE
                                            CONTROLLING AUTHORITY)
EVALAUTH
ADMINISTRATIVE CHAIN OF COMMAND
COMNAVIDFOR SUFFOLK VA
NCMS WASHINGTON DC
SERVICING A&A TEAM
BT
C O N F I D E N T I A L
MSGID/GENADMIN/USS SHELLBACK/-/SEP//
SUBJ/INITIAL REPORT OF COMSEC INCIDENT//
REF/A/NCMS WASH DC/-/-//
AMPN/REF A IS EKMS-1(SERIES)
POC/UNDERWAY, I B/LTJG/USS SHELLBACK/TEL:315-243-2247/EMAIL:
IBUNDERWAY(AT)DDG91.NAVY.MIL//
RMKS/IAW REF A, THE FOLLOWING IS PROVIDED:
1.  427856/TS
2.  USKAT 4389 EDITION F REG 1, SECRET, COMUSFLTFORCOM
3.  RADIO WATCH SUPERVISOR, TS
    RADIO WATCH STANDER, TS
4.  DURING A ROUTINE SPOT CHECK OF THE LE, IT WAS DISCOVERED THAT
ONE OF THE TWO PERSONNEL IDENTIFIED IN PARA (3) HAD DEPARTED THE
SPACE HOWEVER, IT WAS DISCOVERED THAT THE SECURITY CONTAINER IN WHICH
THE MATERIAL IS STORED WAS SHUT BUT NOT PROPERLY LOCKED (BY SPINNING
THE DIAL) AND VERIFIED PRIOR TO SIGNING THE SF-702 AND DEPARTING THE
SPACE.  ACCORDING TO THE SF-702 AND STATEMENTS OBTAINED FROM BOTH
PERSONNEL, A SINGLE PERSON HAD ACCESS TO THE CONTAINER AND STORED
MATERIAL FOR APPROXIMATELY 10 MINUTES.  THE CONTAINER IS LOCATED IN A
RESTRICTED AREA WHERE ACCESS IS CONTROLLED THROUGH A CIPHER LOCK
(WHEN MANNED), AN ACCESS LIST AND VISITORS LOG.  A COMPLETE INVENTORY
WAS TAKEN AND ALL MATERIAL ACCOUNTED FOR AND IN-TACT.  ONLY THE
CURRENTLY EFFECTIVE SEGMENT OF THE ITEMS DESCRIBED IN PARA (2) ABOVE
HAVE BEEN REMOVED FROM THEIR PROTECTIVE PACKAGING (CANISTER) FOR
ROUTINE USE.
5.  PHYSICAL INCIDENT (LOSS OF TPI)
6.  LOCAL COMMAND INQUIRY IN PROGRESS AND TRAINING WILL BE PROVIDED
TO ALL LE PERSONNEL TO REITERATE THE NEED TO ENSURE PROPER SECURITY
PROCEDURES NOT ONLY EXIST BUT ARE FOLLOWED AT ALL TIMES.
```

FIGURE 9-2

7. N/A
8. SAME AS POC ABOVE.
9. A. 07 JUL 2011
   B. 13 SEP 2011
   C. 08 OCT 2011
DERIVED FROM: EKMS-1(SERIES)//
DECL/22SEP2028//

EXAMPLE CLOSING ACTION MESSAGE

FROM: (EVALAUTH)
TO: (VIOLATING COMMAND)
BT
UNCLASSIFIED
MSGID/GENADMIN/NCMS WASHINGTON DC//270-09//
SUBJ/CLOSE-OUT OF COMSEC INCIDENT CA358156 - N50302-09//
REF/A/GENADMIN/USS SHELLBACK/141829ZZJUL09//
REF/B/GENADMIN/DIRNSA/071157ZAUG09//
REF/C/DOC/NCMS WASH DC/05APR10//
NARR/REF A IS USS SHELLBACK INITIAL REPORT OF COMSEC INCIDENT. REF B IS DIRNSA FINAL EVALUATION OF REF A. REF C IS EKMS-1(SERIES)//
POC/U.B. UNDERWAY/IA03/N5/LOC:NCMS WASHINGTON DC/TEL:240-857-7704/EMAIL:ULYSSES.UNDERWAY@NAVY.MIL//
POC/C.U. LATER/IA03/N5/LOC:NCMS WASHINGTON DC/TEL:240-857-7708/EMAIL:CLARENCE.LATER@NAVY.MIL//
RMKS/1. CONCUR WITH FINAL EVALUATION OF NO COMPROMISE.
2. ENSURE MEASURES ARE PUT IN PLACE TO MINIMIZE THE POTENTIAL FOR A REOCCURRENCE.
3. UNLESS ADDITIONAL INFORMATION BECOMES AVAILABLE WHICH COULD CHANGE THIS ASSESSMENT, THIS CASE IS NOW CLOSED.
4. RETAIN THIS MESSAGE AND RELATED REFERENCE DOCUMENTS IN YOUR CORRESPONDENCE FILE IAW REF C.//
BT

FIGURE 9-3

CHAPTER 10 -- PRACTICES DANGEROUS TO SECURITY (PDSs)

CHAPTER 10 - PRACTICES DANGEROUS TO SECURITY (PDSs)

1001. **GENERAL**:

a. PDSs, while not reportable to the national level (NSA), are practices, which have the **potential** to jeopardize the security of COMSEC material, **if** allowed to perpetuate.

b. All accounts must conduct annual PDS familiarization training that will, at a minimum, include reviewing and discussing this chapter. Document training locally in accordance with command directives.

c. There are (2) types of PDSs: Reportable and Non-Reportable. Non-reportable PDSs must be documented at the unit level and reported to the CO of the account but are not reported outside the command. Supported LEs both internal and external must notify the supporting EKMS Manager of all PDSs and incidents to ensure compliance with external reporting timeframes, when required.

1005. **IDENTIFICATION OF PDSs**:

a. **The following is a list of NON-reportable PDSs**:

(1) Improperly completed accounting reports (i.e., unauthorized signatures, missing signatures or required accounting information, incomplete short title information).

(2) Physical COMSEC keying material transferred with status markings still intact.

(3) Mailing, faxing or scanning/emailing (via non-secure fax) SF-153s, CMS-25s or other documents containing status information or marked as classified. If passed electronically via NIPRNET, a report of spillage is required per SECNAV M5510.36 and IA Pub 5239.26.

(4) COMSEC material not listed on account inventory when documentation exists to indicate that the material is charged to the account, **OR** COMSEC material not listed on local element (LE) or user inventory when documentation exists at the account level to indicate that the material was issued to the **LE or user, as applicable.**

(5) Issue of keying material in hardcopy form marked/designated CRYPTO, without authorization, to a LE more

than 30 days before its effective period.

(6) Removing keying material from its protective packaging prior to issue for use, or removing the protective packaging without authorization, as long as the removal was documented and there was no reason to suspect espionage. (See Article 769.g note 1 for exception where premature extraction is not deemed a PDS).

(7) Receipt of a package with a damaged outer wrapper, but an intact inner wrapper.

(8) Activation of the anti-tamper mechanism on or unexplained zeroization of COMSEC equipment as long as no other indications of unauthorized access or penetration was present.

(9) Failure to maintain OTAD/OTAR/OTAT logs.

(10) PIN, Password, Rekey-related non-reportable PDSs:

(a) Failure to perform a KP or STE/SCIP product rekeys annually, or more frequently.
(b) Failure to update and properly record LMD or MGC Passwords (root, sysadmn, opr, etc.. every 3 months).
(c) Failure to change KP CIK Pins every 90 days or more frequently).
(d) Failure to properly maintain KP CIK/PIN log.

(11) Failure to perform LCMS backups or archives in accordance with Article 718.d and Annex X paragraph 12.s.

(12) The discovery of non-COMSEC accountable material in LCMS.

(13) Loss or finding of unclassified material as defined in Article 1015.

(14) Failure to report either the receipt of COMSEC material or corrupt Bulk Encrypted Transactions (BETs) within 96 hours of receipt or download, as applicable.

(15) Failure to submit and retain on file inventory completion messages. **Not applicable to inventories used solely for Change of Command**.

(16) Failure to conduct, document and retain either

semi-annual self-assessments or required spot checks.

(17) Failure to report via record message LMD/KP failures 07 days or greater in duration.

(18) Loss of User CIKS for INEs or devices which make use of CIKS. The CIK or card association, as applicable must be deleted promptly from the device. If the associated device is lost or was possibly accessible to unauthorized/improperly cleared personnel submit a COMSEC incident report in accordance with Article 945.e.

(19) Failure to inventory affiliated DTD, SKL, and TKL CIKs during inventories.

(20) Failure of a LE to conduct, document and retain inventories for Change of Command or Change of LE Issuing.

NOTE: Although the PDS identified in (13) above is categorized as non-reportable, NCMS must be contacted to effect replacement or obtain disposition instructions for loss/found item. A sample non-reportable PDS memorandum can be found in Figure 10-1.

AMD-9

(21) Failure to conduct, document, submit and retain account-level inventories, as applicable and self-reconcile the accounts inventory within the specified time frames unless an extension is granted by NCMS in writing. This includes the inventory of both ALC 4 and ALC 7 material which is locally accountable to the EKMS account.

SAMPLE NON-REPORTABLE PDS MEMORANDUM

03 Apr 2014

MEMORANDUM

From: EKMS Manager (or Alternate) USS Blue Horse
To: Commanding Officer, USS Blue Horse
Via: (as applicable with command administrative procedures)

Ref: (a) EKMS-1(series)
(b) EKMS-3(series)

Subj: DOCUMENTATION OF THE DISCOVERY OF A NON-REPORTABLE PDS

1. On 02 April 2014 during the conduct of a CO’s Spot Check, (2) accounting reports (TN 000047, TN 00096) were discovered in the Chronological File which were not signed by two personnel, as required per reference (a).

2. The above deficiency constitutes an incomplete accounting report and per reference (a) must be documented and brought to the attention of the unit CO.

3. A review of all active accounting reports will be conducted to identify any additional accounting reports still required to be retained which may not have been properly completed. If discovered, the matters will be properly documented and brought to your attention.

4. A copy of this memorandum will be affixed to the accounting reports reflected in paragraph (1) above.

Very Respectfully
I. B. INTROUBLE

Copy to:
Account XXXXXX PDS/Incident File
XXXXXXXXXXX (LE/work center)

Figure 10-1

b. **The following PDSs must be reported OUTSIDE the command as indicated in Article 1010**:

(1) For physical material, if the material was not destroyed but was erroneously flagged and confirmed as destroyed within LCMS, the unit must request assistance from a COR Manager at NCMS to return the material to proper accountability.

NOTE: If material is not lined-out and initialed on the destruction report to indicate the material was not destroyed this will be considered a COMSEC Incident IAW Art. 945.e.6.

(2) Unauthorized adjustment of preconfigured default password parameters on LMD (e.g. LCMS SCO password lockout and/or reset). See Article 515.i for details.

(3) Failure to return a Key Variable Generator (KVG), i.e. KG-83, KGX-93, or KP for recertification within 30 days of receipt of a replacement unit.

NOTE: (1) If deployed and unable to enter the device into DCS for shipment, the unit will notify the COR, NCMS and CMIO Norfolk via message requesting a waiver to the policy above and will provide an anticipated shipping date. Once shipped, notification to the recipient will be in accordance with Article 535.o.

(2) There is no recert requirement for KOK-22A TESTPACs.

1010. REPORTING AND DOCUMENTATION REQUIREMENTS:

a. All other PDSs will be documented (locally) or reported externally, as applicable no later than 72 hours from the time of discovery.

b. PDS 1005.b (2) must be reported outside the command as follows:

TO: NCMS WASHINGTON DC//N3/N5//
INFO: ISIC
COMNAVIDFOR SUFFOLK VA
Servicing A&A Team

SUBJ: REPORTABLE PDS UNAUTHORIZED ADJUSTMENT
OF PRE-CONFIGURED DEFAULT PASSWORD

PARAMETERS ON LMD (LCMS SCO PASSWORD
LOCKOUT AND/OR RESET)

(1) EKMS ID Number and HCI

(2) List the unit POC

(3) Provide the circumstances surrounding the cause of non-compliance. Include an estimate of the length of time of non-compliance.

(4) List corrective measures taken to preclude reoccurrence.

f. PDS 1005.b.(3) must be reported outside the command as follows:

TO: NCMS WASHINGTON DC//N3/N5//
INFO: CMIO NORFOLK VA
COMNAVIDFOR SUFFOLK VA
Reporting Units ISIC
Servicing A&A Team

SUBJ: LATE RETURN OF A KEY VARIABLE GENERATOR (KVG)

(1) EKMS ID Number and HCI.

(2) List the unit POC.

(3) Identification of the material (i.e., short title, and serial number

(4) The expiration date on the device.

(5) Reason for the delay.

1015. <u>REQUESTING DISPOSITION FOR THE LOSS OR FINDING OF UNCLASSIFIED COMSEC MATERIAL</u>:

a. The loss or finding of the following unclassified material is considered a NON-REPORTABLE PDS; however, NCMS must be contacted to effect replacement of missing item or to obtain disposition instructions for found item.

(1) Unclassified COMSEC equipment and/or related devices <u>not</u> designated CCI.

(2) Unclassified COMSEC-related information such as publications, maintenance manuals, or operating instructions.

(3) Unclassified keying material not marked or designated CRYPTO.

b. Submit a facsimile, letter, or message as follows:

TO: NCMS WASHINGTON DC//N3/N5//
The applicable COR
INFO: CMIO NORFOLK VA//N3//

NOTE: Other addressees as directed by the chain of command

SUBJ: REPLACEMENT OF MISSING UNCLAS MATERIAL **OR** REQUEST FOR DISPOSITION INSTRUCTIONS FOR FOUND UNCLAS MATERIAL

REF/A/DOC/NCMS WASH DC/-//

AMPN/REF A EKMS-1(SERIES) ARTICLE 1015//

RMKS/1. IAW REF A, THE FOLLOWING IS SUBMITTED:

(1) EKMS ID NUMBER.

(2) Identity of material (i.e., short title, edition, accounting (serial or register) number, CONAUTH or promulgating authority).

(3) If applicable, date material needed.

(4) If applicable, specify DCS or other activity for delivery of material, or indicate OTC pickup from a CMIO.

CHAPTER 11 -- MANAGEMENT OF ELECTRONIC KEY

a. General
b. Keying
c. KP CIKs
d. REINIT 1 and NAVREINIT 2 Keys
e. Certification
f. Reporting Zeroized KOK-22s/KPs
g. Emergency Protection

CHAPTER 11 - MANAGEMENT OF ELECTRONIC KEY

1101. INTRODUCTION:

a. The procedures described in this chapter and in NAG 16 (series)[3], Field Generation and Over-the-Air Distribution of COMSEC Key in Support of Tactical Operations and Exercises, describes a joint standard for conducting over-the-air distribution (OTAD). These techniques and methods are consistent with allied procedures contained in ACP 132 (series) and will effectively support combined as well as joint operations.

b. When properly implemented, OTAD procedures improve operational key management flexibility, improve security through greater use of locally generated key, and reduce reliance on logistically unsupportable paper-based systems. Use of OTAD will also increase personnel awareness in proper handling and safeguarding techniques for electronic key.

1102. PURPOSE:

a. This chapter describes the policies and procedures for generating, handling, safeguarding, and distributing 128-bit electronic COMSEC key.

b. NAG 16 (series) is prescribed as the standard user's manual for planning and conducting electronic key generation, over-the-air rekeying (OTAR), and over-the-air key transfer (OTAT).

c. Procedures detailed in this chapter:

(1) **Supplement** those contained in NAG 16 (series).
(2) Address requirements that are DON unique.
(3) Provide a basis for standardization within DON.

d. For ease of use, some of the basic doctrine for OTAR/OTAT in NAG 16 (series) is repeated in this chapter.

e. See Article 1184 for information that is not addressed in this chapter, but contained in NAG 16 (series).

[3] NAG 16 is held by tactical forces of all U.S. services and its combined equivalent, ACP-132, is held by tactical military forces of Australia, Canada, New Zealand, the United Kingdom, and by some U.S. tactical forces.

NOTE: 1. NAG-16 is not COMSEC accountable, may be reproduced locally without authorization and can be obtained from the

2. NAG-16(series) is available for Marine Corps units through the Marine Corps Publication Distribution System (MCPDS).

3. Foreign release of NAG-16(series) requires pre-approved from DIRNSA (Code DP02).

1105. SCOPE:

a. Military commanders at all levels are authorized to direct field generation and distribution of electronic COMSEC key to support operations or exercises and are encouraged to do so.

b. While procedures herein primarily address DON requirements, utilization of electronic key procedures are applicable to U.S. joint and intra-service operations and exercises, and can also be used with allied units[4] that have OTAR/OTAT capable crypto-equipment.

c. Procedures in this chapter apply to fleet broadcasts, point-to-point circuits, and multi-station nets.

d. Electronic key may be converted from key tape or generated by certified KG-83/KGX-93/93A key variable generators, by KY-57/58/67 (VINSON/BANCROFT), KYV-5/KY-99/99A (ANDVT) equipment, and the KOK 22/22A (Key Processor (KP)).

e. Electronic key may be distributed electronically via OTAR or OTAT or physically in a fill device (FD).

1110. LIMITATIONS:

a. Detailed policies/procedures for Joint Tactical

[4] Allied units that use OTAR-capable, "S" nomenclature (special purpose), COMSEC equipment may receive traffic encryption key (TEK) via OTAR, but are not authorized to serve as net control stations (NCSs) for combined nets and circuits that distribute electronic key via OTAR. NAG-22, Over-the-Air Rekeying of Combined Tactical Nets, was produced to explain OTAR and OTAT to these allies. U.S. tactical forces and allied tactical forces that hold ACP-132 do not need NAG-22.

Communications System (TRI-TAC) and Mobile Subscriber Equipment (MSE) secure communication systems are not contained in this chapter. See NAG 16 (series) for more detailed guidance.

b. Procedures herein address routine operational practices, but exceptions are authorized under **COMSEC emergencies** (i.e., the only viable alternative being plain text communications) as determined by the CO/on-scene commander. Implementation of other than prescribed procedures must be in support of an urgent and unforeseen operational requirement and not become routine practices.

1115. RESPONSIBILITIES:

a. Field generation and electronic distribution are the **preferred** means for providing electronic key to DON tactical forces. Commanders responsible for key provisioning to such forces should endeavor to produce locally the tactical 128-bit key required and distribute it via over-the-air key distribution (OTAD). Specifically, commands authorized a KG-83 or KP are expected to employ locally generated key to support limited scale operations. Holders ashore will generate TEK for point-to-point circuits as well as KEK where the electronic KEK can be physically transferred in a FD to authorized recipients. Additional guidance follows:

(1) Carrier battle group and amphibious ready group commanders should establish OTAR-capable, intra-force and embarked amphibious force nets/circuits using a start-up KEK, should generate group required OTAR TEKs with the KG-83 or KP allocated to their flagships, and OTAR the generated key to ships in company.

(2) Marine forces should generate OTAR TEK for their KY-57/58/67 and KYV-5/KY-99/99A secured nets/circuits at the NCSs and distribute them via OTAR and generate other 128-bit tactical key in KGX-93/93A TRI-TAC key variable generators (KVGs), if available.

(3) The commander who directs field generation of electronic key becomes its CONAUTH; see Annex C of this manual. Electronic key converted from tape key remains under the purview of the designated CONAUTH.

(4) Submarine commanders and any commander who regularly holds material in excess of normal reserve on board (ROB) should employ OTAD to reduce holdings of material that

historically have been used sparsely.

b. EKMS Manager personnel are not required to supervise or witness the generation, relay, transfer, receipt, or destruction of locally generated electronic key. Any personnel who are fully qualified and authorized access to COMSEC keying material may execute these actions.

c. EKMS personnel are responsible for overseeing the implementation of and compliance with this chapter (e.g., a periodic review of local logs, adherence to TPI requirements).

1120. DEFINITIONS:

Definitions and commonly used abbreviations/acronyms in this chapter are contained in Annexes A and B, respectively.

1125. CRYPTO-EQUIPMENT CAPABILITIES:

U.S. crypto-equipment capable of field generating electronic key and/or distributing it over the air is identified in NAG-16(series).

1130. TYPES OF KEY:

The principal types of key covered in this chapter are as follows:

a. **Key Encryption Key (KEK)**: Key that encrypts or decrypts other key for transmission or storage.

b. **Start-Up KEK**: Key encryption key held in common by a group of potential communicating entities and used to establish ad hoc tactical nets.

c. **Traffic Encryption Key (TEK)**: Key used to encrypt plain text or to super encrypt previously encrypted text and/or to decrypt cipher text.

1140. SAFEGUARDING REQUIREMENTS FOR KEYED CRYPTO-EQUIPMENT:

a. TPI safeguards are not required for TOP SECRET keyed COMSEC equipment located in spaces that are **continuously** occupied by appropriately cleared persons who are in sight of each other **and** the keyed equipment.

b. Keyed COMSEC equipment used to terminate part-time nets/circuits may be left in unattended spaces, provided the equipment has been rekeyed by OTAR or updating with the next future TEK immediately before terminal close-down. Reasonable security measures must be taken (e.g., locking a door and controlling access) to prevent theft, tampering, or unauthorized operation of a keyed terminal when unattended.

c. Keyed COMSEC equipment used to terminate full-time nets/circuits may be left in unattended spaces only if such spaces meet DON criteria for open storage of information classified at the same level of the TEK used.

1145. CERTIFYING AND HANDLING KEY VARIABLE GENERATORS (KVGs):

NOTES: 1. See Article 1185 for KP certification requirements.

2. Commands desiring instructions on how to properly inspect tamper evident seals placed on certified equipment or any other protective packaging technologies are encouraged to contact their servicing ~~CMS A&A~~ COR Audit Team.

AMD-9

a. KG-83s have been distributed to afloat and shore commands in accordance with the KG-83 Master Plan. KG-83 KVGs are used by the Navy and Coast Guard to generate OTAR TEK for use with KG-84A/84C secured nets and circuits. KGX-93/93A KVGs are used by the Marine Corps to generate key for TRI-TAC switches.

b. KG-83 and KGX-93/93A KVGs used to produce operational key must be certified prior to initial use, at least every two years thereafter, following maintenance, and whenever security control is lost (e.g., KVG is found outside of proper storage and unattended). This certification process provides the necessary assurance that the equipment is functioning according to design specifications.

NOTE: There are no certification requirements for KY-57/58/67 and KYV-5/KY-99/99A equipments.

c. Certification must be performed by one qualified technician using NSA prescribed routines and KT-83 test equipment.

d. All KG-83 and KGX-93/93A KVGs will be certified to the

SECRET level and all certified KVGs having all tamper detection labels intact are authorized to generate 128-bit keys for any purpose, at all classification levels. KPs are authorized to generate 128-bit key for any purpose, up to the classification level to which they have been certified/privileged.

e. Marine Corps elements are responsible for certifying their own KGX-93/93As. Marine Corps KGX-93/93As are certified and repaired by Electronic Maintenance Companies (ELMACO), Communications Battalions (CommBns), Communications Squadrons (CommSqs), and Communications Companies (CommCos).

f. NCCOSC RDTE DIV CRF San Diego is the primary location for recertification of KG-83s. SPAWARSYSCEN ATLANTIC Charleston has been tasked to manage the certification of KG-83 devices. This includes maintenance of a database containing all KG-83 devices within DON, serial numbers, holder, and recertification dates. The database program automatically identifies those KG-83 devices requiring recertification.

(1) Due to a two-month certification pipeline, all KG-83s will enter the certification process two months prior to expiration. NCCOSC RDTE DIV CRF San Diego will notify the holder by message that a replacement KG-83 has been forwarded. Upon receipt of the new KG-83, the holder will remove the old KG-83 from service and pack and ship the old KG-83.

(2) If a KG-83's certification is scheduled to expire within **30 days** and a replacement KG-83 has not been received, the using command must notify by message SPAWARSYSCEN ATLANTIC CHARLESTON SC//722//, Info NCMS WASHINGTON DC//N3//, the using command's ISIC and operational commander).

(3) If a KVG's certificate expires while its user is awaiting delivery of a certified replacement, the user may continue to use the affected KVG and should **not** report the situation as a COMSEC incident.

g. If a KG-83 or KGX-93/93A fails, the using command must request a certified replacement by message from ATLANTIC CHARLESTON SC//722//, INFO NCMS WASHINGTON DC//N3//, the using command's ISIC and operational commander. While waiting for a replacement, the using command should continue to operate the affected nets/circuits by selecting one of the following alternatives if no KP is available:

(1) Continue OTARing by taking a DTD (AN/CYZ-10 or

AN/PYQ-10) to the closest certified KG-83 or KGX-93/93A and fill it with up to 1000 unique 128-bit OTAR TEKs.

NOTE: Each carrier battle group and amphibious ready group flagship holds a KG-83, and approximately 13 Marine Corps tactical commands hold KGX-93/93As.

(2) Continue OTARing by implementing contingency, one-copy OTAR TEK tape keys, if held.

NOTE: Shore command KG-83 users must hold enough contingency OTAR TEK to support OTAR operations for a month if their KVGs fail, but tactical KG-83 and KGX-93/93A users are not required to hold back up key.

(3) Temporarily revert to traditional keying, by shifting affected OTAR KEKs to non-OTAR TEKs having monthly cryptoperiods and updates each working day. When a certified KVG becomes available, this temporary arrangement must be terminated with the affected non-OTAR TEKs reverting to OTAR KEKs with 3-month cryptoperiods.

h. After each KG-83 or KGX-93/93A certification or recertification, certifying personnel must apply NSA-furnished tamper detection labels in accordance with NSA instructions. Certifying activities must record the serial numbers of the labels they apply to each KVG so that this information may be provided to investigating elements if tampering is ever suspected. Recorded label serial numbers must also be compared with those removed from each KVG at recertification. Any unexplained differences must be reported as a COMSEC incident.

i. Each certified KG-83 or KGX-93/93A must be tagged on a handle to show its classification, "CRYPTO" status, date of certification, command that performed certification, and name and rank of certifying technicians. Such tags are to be prepared locally at certification sites and are to be tied securely to one of the KVG handles.

j. Users of KG-83s and KGX-93s must examine applied tamper detection labels immediately before KG-83 or KGX-93/93A activation. Detection of a damaged label invalidates a KVG’s certification and must be reported as a COMSEC incident (see Chapter 9). The affected KVG must then be recertified.

k. Certified KG-83s must be stored as SECRET COMSEC material under no-lone zone (NLZ) at repair sites. When installed in operational communications environments, certified KG-83s need not be afforded TPI or NLZ protections, provided their “dutch doors” are double-locked with TPI-approved combination locks.

l. Certified KGX-93/93As must be stored as SECRET COMSEC material at recertification sites.

m. Certified KG-83s and KGX-93/93As must be shipped using any of the methods approved in Article 530 for SECRET COMSEC equipment.

n. When installed in TRI-TAC switches, two authorized persons using the two-person access lock must lock certified KGX-93s, to which tamper detection labels have been applied into place. Provided that this is accomplished, certified KGX-93s need not be removed when their locked shelters are left unmanned.

o. Decertified KG-83s and KGX-93/93As, including those being returned for certification, must be handled as CONFIDENTIAL COMSEC material and may be shipped via U.S. registered mail provided THAT it does not pass through a foreign postal system or foreign inspection, Defense Courier Service (DCS), Cleared Commercial Carriers using Protective Security Service, or U.S. military contract service (e.g., AMC, LOGAIR, QUICKTRANS).

NOTES: 1. Registered mail sent to an FPO AE/AP address does NOT pass out of U.S. control.

2. In <u>COMSEC emergencies</u>, a KVG with an expired certification may be used, pending recertification or replacement.

1150. <u>SOURCES OF ELECTRONIC KEY</u>:

NOTE: The types and sources of key associated with OTAD/T can be found in NAG-16(series). Abbreviated information on these keys is provided herein for ease of use.

a. **<u>KEK</u>**:

(1) Normally produced in tape form and held at using locations. However, when all users are located close enough to the producer/source it may be field-generated and delivered in FDs.

(2) **In COMSEC emergencies**, any uncompromised, classified key that is held in common by affected commands and that is not used for any other purpose may serve temporarily as KG-84A/84C/KIV-7, KY-57/58/67, or KYV-5/KY-99/99A KEK, until properly classified KEK can be provided.

b. **TEK**:

(1) Generated electronically by an authorized KVG[5],

converted from tape key, or held in tape form. KVGs may generate 128-bit TEK for any of the COMSEC systems listed in NAG 16.

(2) **In COMSEC emergencies**, any uncompromised, classified key that is controlled by the using NCS and that is not used for any other purpose may be used as OTAR TEK.

NOTE: Except in COMSEC emergencies, TEK generated by KY-57/58/67 and KYV-5/KY-99/99A equipment is restricted to use in their respective cryptosystem families.

c. **Start-up KEK**:

(1) Normally produced in tape form or converted from tape to electronic form and delivered physically in FDs.

(2) **In COMSEC emergencies**, individual segments of start-up KEK may be distributed via OTAT.

NOTE: KEK, TEK, and start-up KEK are used in cryptonets operating with KG-84A/84C/KIV-7, KY-57/58/67, and KYV-5/99/99A equipments only.

d. **KW-46 Key**: The KW-46 uses three types of key:

(1) Broadcast Area Variable (BAV) produced in tape form and delivered to users encrypted in that unit's unique variable.

(2) Unique Variable (UV) produced in tape form.

[5] To the maximum extent possible, military commanders should field-generate the TEK needed to support their operations and exercises.

NOTE: The EKMS Manager must ensure that the reg/serial numbers of the BAV and UV match for the respective editions. If they do not, report the discrepancy to NCMS and info CMIO Norfolk.

(3) Community Variable (CV) produced in tape form, but may also be generated by certified KG-83/KGX-93/93A KVGs or converted from tape key and distributed in a FD or electronically via OTAR/OTAT.

NOTE: See NAG-16(series) for additional information on the use of KW-46 keys and OTAR/OTAT communications procedures.

e. **General Guidance**:

(1) Carrier battle groups and amphibious ready group commanders should establish OTAR-capable, intra-force nets and circuits using a start-up KEK, generate DON OTAR TEKs with the KG-83 KVG or KP allocated to their flagships, and distribute the keys to ships in company via OTAR. Carrier battle groups and amphibious ready groups are encouraged to requisition their own start-up KEKs, so that a start-up KEK having the smallest distribution may be used to create tactical nets/circuits.

(2) Marine forces should generate OTAR TEK for their KY-57/58/67 and KYV-5/KY-99/99A secured nets and circuits at the respective NCSs and distribute them via OTAR.

(3) Navy and Coast Guard broadcast stations should generate and distribute via OTAT the key required by ships and afloat commanders they support.

1153. GENERATION OF KEY BY FIELD SITES:

a. **KG-83 and KGX-93/93A KVGs**:

KG-83/KGX-93/93A KVGs are authorized to generate 128-bit key up to the TOP SECRET level. Key generated by these equipments are authorized for use with any crypto-equipment that uses 128-bit key.

NOTE: SCI/SI cleared personnel may use KG-83/KGX-93/ KGX-93A equipment located in GENSER spaces to generate 128-bit key for use on SCI/SI protected circuits.

b. **KY-57/58/67 and KYV-5/KY-99/99A**: **Except in COMSEC emergencies**, key generated by these equipments is restricted to use in their respective families.

1155. CLASSIFICATION OF ELECTRONIC KEY:

a. **Field-generated electronic key**, while not physically marked with a classification, must be handled and stored based on the highest classification of information to be protected or the TEK being passed.

b. **Electronic key converted from tape key** must be handled and stored at the same level of classification as the tape key from which it was converted.

c. **In COMSEC emergencies**, classified electronic key may be used to secure information classified one level higher than its classification.

1160. ALLOCATION OF ELECTRONIC KEY:

a. **OTAR KEK** must be allocated as follows:

(1) Point-to-Point (PTP) circuits:

(a) Each PTP circuit that is secured by KG-84A/84C/KIV-7s, KY-57/58/67s, or KYV-5/KY-99/99A must use a unique short title of KEK.

NOTE: For security reasons, it is important that multiple KG-84A/84C/KIV-7 secured PTP circuits that terminate in the same NCS be keyed with separate OTAR TEK and not with a common OTAT TEK, as would be appropriate for multiple-station radio nets in tactical environments.

(b) For parallel KG-84A/KG-84C/KIV-7 secured circuits terminating in the same space at both terminals, the same short title may be used with the parallel circuits, but separate segments (physical or electronic) must be used for each circuit.

NOTE: In COMSEC emergencies, a common KEK may be used for all PTP circuits controlled by a NCS, until separate, two-copy KEK can be provided for use with each out station (OS).

(2) Multi-station nets:

(a) The NCS for each multi-station net that distributes TEK via OTAR must specify whether OTAR will be accomplished sequentially (i.e., one OS at a time) or simultaneously for all net OSs (see NAG 16 (series)).

(b) If a NCS uses the sequential method, each OS must have a unique KEK short title.

(c) All net OSs must hold a common KEK (or start-up KEK) when the simultaneous method is used.

NOTE: Creation of a net with start-up KEK automatically provides a common KEK for all net OSs and mandates simultaneous OTAR.

b. **OTAR/OTAT TEK** must be allocated as follows: A unique segment of OTAR TEK or a unique, field-generated OTAR TEK must be used on each KY-57/58/67, KG-84A/84C/KIV-7, or KYV-5/KY-99/99A secured net/circuit.

c. **Start-up KEK** must be allocated as follows:

(1) Each edition of start-up KEK is produced in the "VA" format (62 segments, daily cryptoperiod) and is effective for two months.

(2) Segment use is based on a predictable day/date relationship (e.g., segment 5B may be used only on the fifth day of the second month that an edition is effective). Segments 1A - 31A are used during the first month, and segments 1B - 31B are for use during the second month.

(3) Each segment of start-up KEK is effective for only one radio day. During that day, any tactical commander who holds a KYX-15 or DTD (AN/CYZ-10 or AN/PYQ-10) may use the effective segment to activate any number of OTAR-capable nets or circuits (see NAG 16 (series)).

NOTE: Use of start-up KEK is limited to tactical forces requiring the establishment of temporary circuits or nets in support of temporary operations/exercises.

1165. DISTRIBUTION OF 128-BIT ELECTRONIC KEY:

a. **KEK:**

(1) Distribute physically in tape form or by FD after electronic conversion/generation or via OTAT using DTDs on a

STE-secured circuit. (See Article 1165.e. for details.)

(2) In shore establishment environments where the same EKMS account distributes OTAR KEK to all members of a complex of KG-84A/84C/KIV-7 secured PTP circuits (e.g., an NAS supporting aircraft squadrons), it is not necessary to procure tape OTAR KEK to link each OS with the NCS. A unique OTAR KEK for each link can be extracted from a certified KVG or generated from the LMD/KP and delivered quarterly to each OS in a FD or a unique segment of the NCS's OTAR TEK can be allocated to serve as the KEK for each link and be delivered quarterly to each OS.

(3) **In COMSEC emergencies**, KEK and individual segments of start-up KEK may be passed via OTAT until physical distribution in tape form can be arranged. (See Article 1165.e. for sole method approved for OTAT of KEK during non-emergencies.)

b. **TEK**:

(1) To maximum extent possible, distribute TEK electronically via OTAR or OTAT.

(2) If KEK of proper classification is used, any 128-bit tactical TEK may be distributed via OTAT, using STE, DTD terminals[6], KW-46 secured broadcasts, KG-84A/84C/KIV-7, KY-57/58/67, or KYV-5/KY-99/99A secured nets/circuits.

c. **Distribution via KW-46**:

(1) The GENSER broadcast channels are limited to distribution of key protecting GENSER circuits only.

(2) OPINTEL broadcast channels are authorized to distribute key for both GENSER and SCI/SI circuits.

(3) The two Naval Computer and Telecommunications Area Master Stations (NCTAMS) and both NCTS Guam and NCTS Eurcent are authorized to generate and distribute by OTAR and/or OTAT the KW-46 CVs that are required to support the U.S. surface broadcast channels they originate. However, worldwide back-up CVs (one each for GENSER and SCI/SI) will be retained in contingency status for use in the event of some unforeseen

[6] Any tactical TEK may be transmitted via OTAT using the secure mode of STU-III/STE secured telephone circuits having DTDs (AN/CYZ-10s or AN/PYQ-10) attached.

requirement.

(4) KW-46 CVs that are field-generated or converted from tape may be distributed on KW-46 secured broadcasts via OTAT for extraction via a FD or via OTAR for use in the receiving KWR-46.

NOTE: Extraction of key from a KW-46 receive terminal is restricted to authorized recipients only. All broadcast subscribers must zeroize their KW-46 extraction registers immediately after completion of key transfer. Key that is received via OTAT in the UVRQ/Rekey register that is not intended for use by a command may be zeroized by a <u>single</u> operator.

d. **<u>SCI/SI Key restrictions</u>**:

(1) Except when specifically authorized by the CONAUTH, OTAT of SCI/SI TEK is restricted to transmission via circuitry protected by SCI/SI key.

(2) Procedures established by the CONAUTH for passing SCI/SI key in other than SCI/SI protected circuits must be <u>strictly</u> followed to preclude the possible compromise of SCI/SI information.

e. **<u>OTAD of Key via STE</u>**:

(1) When connected to a DTD (AN/CYZ-10 or AN/PYQ-10), a STE terminal may be used to transfer unencrypted (red) strategic key and tactical key of all classifications and categories, and their associated key tags, to a distant STE so configured.

NOTE: Per the Operational Security Doctrine, TrKEK may not be OTAT'D in red (unencrypted form) via STE except in an emergency. TrKEK must be pre-encrypted prior to transfer via STE.

(2) Each of the communicating STEs must meet the following requirements:

(a) Be in the secure data mode that is equal or higher than the classification level of key being transferred.

(b) A NSA-approved connector cable and cable adapter must be used between the terminal and the DTD.

(c) The DTD must use NSA's standard STE compatible fill/CT3 application software package.

(d) Have a unit-specific department/agency/ organization (DAO) description on the second line of their non-scrolling STE display.

(e) Article 1165.a. (and NAG 16 (series)) which prohibits OTAT of KEK does **not** apply when a KEK is passed between DTDs on a STE-secured circuit.

NOTE: An example of a unit-specific DAO description is "USS WEST VIRGINIA." To prepare for OTAT, units that do not have unit-specific DAO descriptions should order new STE key associated with such descriptions. For more information on DAO descriptions, see EKMS 702.01.

(3) See NAG-16(series), for the procedures for transferring key and tag from one DTD to another via STE.

f. **Distribution of BETs/IETs via SIPRNET**:

(1) Disks containing only EKMS BETS/IETS may be transmitted as attachments over SIPRNET electronic mail. In doing so, EKMS Managers must ensure compliance in regard to obtaining CONAUTH approval.

(2) EKMS Managers are to ensure that the provisions for transferring, accounting, and destruction of key via floppy diskettes are followed in accordance with Article 769.i.

AMD-9 (3) Procedures to perform distribution via the SIPRNET can be obtained by contacting the local ~~CMS A&A~~ COR Audit Team supporting the region of the account.

NOTE: This procedure is not intended to replace existing methods for transmitting electronic key (e.g., X.400 Direct Communications), or removable media (e.g., floppy disks), but provides an alternative communications path when normal delivery means cannot be used. NSA Central Facility will not authorize this method of transmitting electronic key as a matter of routine practice.

1166. TIMING OF OTAT KEY DISTRIBUTION:

Key may be distributed via OTAT at any time during its effective cryptoperiod, and the cryptoperiod immediately preceding that in which it is to become effective (e.g., weekly cryptoperiod KG-84C TEK that is generated by a field station may be passed anytime during the week preceding its intended implementation).

1170. NOTIFICATION OF IMPENDING KEY TRANSFER (OTAT):

a. A transmitting station must notify all recipients of key to be passed via OTAT prior to the actual transmission of key.

b. The notification must include the following:

(1) Time key will be transmitted.

(2) Identity of the circuit on which key will be sent.

(3) Destination instructions for recipients (i.e., device/circuit for which the key is intended).

(4) Identification of the key to be transmitted, to include short title, classification, effective period, and Controlling Authority.

1175. TAGGING/IDENTIFICATION OF OTAT KEY:

a. Electronically generated key for transmission via OTAT must be tagged or marked to allow immediate recognition of the key. A tag or designator will be assigned to key by the generating station. LMD/KP generated key will be tagged by the LMD.

(1) Tagging field-generated key: The generator of the key will tag the key by using three fields of information. Each field and its description will be as follows:

(a) **Field 1**: A two-digit number that represents the number of electronic keys produced by the generating station. It is assigned in a one-up sequence and will restart daily at 0001Z.

(b) **Field 2**: This field will identify the CONAUTH.

(c) **Field 3**: The Julian date the key was generated.

EXAMPLE: "01C7FLT365" - 01 represents the first key generated. C7FLT represents COMSEVENTHFLT, and 365 represents the Julian date the key was generated.

NOTE: Key tags should not exceed ten characters (i.e., letters/numbers).

(2) **Tagging key converted from tape key**: Electronic key converted from tape key will be tagged by using four fields of information. Each field and its description will be as follows:

(a) **Field 1**: Identification of key as either Allied (A) or U.S. (U).

(b) **Field 2**: Identification of the four to six digits of the short title.

(c) **Field 3**: One or two-letter identification of the edition.

(d) **Field 4**: Two-digit identification of the segment number.

EXAMPLE: "U1019BC07" - U for USKAT, short title 1019, edition BC, segment 07.

b. **Additional identification requirements**:

(1) In addition to the tagging of electronic key, the transmitting station must notify all recipients in advance of transmitting the key and provide the information contained in Article 1170.

(2) All commands that handle electronic key will, as required, maintain local accounting records and clearly label the identity of key contained in FDs. Article 1182 contains procedures for maintaining local accounting records.

1176. HANDLING OF KEK AND TEK:

a. **KEK**: Each tape segment and/or its electronic equivalent, held in a FD, may be used only on its designated circuit and must be destroyed no later than 12 hours after the end of its cryptoperiod.

b. **TEK**: Each tape segment and/or its electronic equivalent held in a FD, including the DTD when used as a common FD, must be destroyed or zeroized after completing an operation successfully in accordance with the following:

(1) Relay stations must zeroize their FDs immediately after confirming successful relay of OTAT key.

(2) End users of key, except for NCTSs and NCTAMSs in KG-84A/84C/KIV-7, KY-57/58/67, or KYV-5/KY-99/99A nets, should normally destroy their TEK held in FDs immediately after establishing communications, but are authorized to retain TEK held in FDs throughout the effective period of the key if required for operational purposes. The TEK must be destroyed no later than 12 hours after the end of its cryptoperiod.

(3) NCSs and NCTAMSs for KG-84A/84C/KIV-7, KY-57/58/67, or KYV-5/KY-99/99A nets are authorized to retain OTAT TEK in tape form when electronic key is converted from tape key and its electronic equivalent in a FD throughout its effective cryptoperiod. The key, all forms, must be destroyed no later than 12 hours after the end of its cryptoperiod.

c. **NON-OTAR TEK Destruction:**

Operational requirements to retain KG-84 and KIV-7 TEK for use later in a cryptoperiod should be accommodated by use of redundant segment tape format (e.g., 5 copies of 6 unique keys monthly cryptoperiod). After extracting it from its canister, a user may retain the last redundant tape segment of such TEK until superseded (retain IAW Article 772). This easement does not apply to tape segments from short titles that are not produced in one of the redundant formats.

1177. **ELECTRONIC KEY STORAGE**:

a. Key may be stored as follows:

(1) In the LMD in encrypted form until operationally required or superseded.

(2) Recipients of physical transfers of key loaded in a FD passed from one person to another are authorized to store key in their FDs until operationally required.

(3) Recipients, less relay stations, of key passed via OTAT are authorized to store key in their FDs until operationally required.

(4) Relay stations must destroy/delete key in their

fill devices within 12 hours after confirming a successful OTAT relay.

(5) NCSs and NCTAMSs for KG-84A/84C/KIV-7, KY-57/58/67, or KYV-5/KY-99/99A/KY-75 nets are authorized to retain TEK, tape and/or electronic, throughout its effective cryptoperiod.

b. TEK and KEK may be used/stored in the same FD.

c. Unencrypted TOP SECRET key stored in a common FD must be afforded TPI handling/storage as required by Article 1135. The key will be destroyed/deleted no later than 12 hours after the end of its cryptoperiod.

NOTE: Exceptions to the 12-hour destruction requirement are reflected in Article 540.

1178. CRYPTOPERIODS FOR KEK AND TEK:

a. **KEK**: The maximum cryptoperiod for each segment of KG-84A/84C/KIV-7, KY-57/58/67, or KYV-5/KY-99/99A KEK, except for start-up KEK, is three months. CONAUTHs may extend cryptoperiods for up to seven days without report. Longer extensions must have prior NSA approval or be reported as a COMSEC incident.

NOTE: Each segment of KG-84A/84C/KIV-7 KEK has a maximum cryptoperiod of three months even if it is drawn from an edition that is then routinely superseded. The U-variable (KEK) is valid for three months however, per NAG-53(series) KG-84A/KIV-7 OTAR KEK in physical or electronic form which has been used must be destroyed within 12 hours of loading. Subsequent cold-starts requires that the next-up segment be loaded. Retention of used KEK is a COMSEC incident per NAG-53.

b. **TEK**: One month is the normal cryptoperiod for KG-84A/84C, KY-57/58/67, and KYV-5/KY-99/99A TEK used on tactical nets/circuits that operate continuously while they are active (i.e., that do not close down for specified periods).

NOTE: See NAG-16(series) for additional information on TEK cryptoperiods.

1179. KEY TAPE ORDERING:

For guidance in ordering key tape (e.g., TEK for OTAR, KEK, and start-up KEK), see NAG 16 (series).

1180. PHYSICAL TRANSFER OF ELECTRONIC KEY IN A FD:

a. The physical transfer of electronic key refers to the exchange of key in a FD from one person to another for use at another location at the same command or a different command. Transfer of key in this manner is authorized provided that the recipients are properly cleared and authorized to hold the key.

NOTE: The transfer of key to a non-authorized holder must be approved by the CONAUTH of the key.

b. Recipients of electronic key in a FD must acknowledge receipt of the key by signing a local custody document. See Article 769.h.(1).

(1) Thereafter, each location holding the key must properly safeguard and continuously account for the loaded FD by serial number until the key is zeroized, overwritten, or otherwise destroyed.

(2) Minimum accounting information for the key must include the short title(s) or designator of the key, date of generation/loading, number of copies made, date of transfer, identity of issuers and recipient, EKMS ID number and the serial number of FD.

1181. INVENTORY REQUIREMENT FOR ELECTRONIC KEY:

a. There is no shift/watch-to-watch inventory requirement for electronic key issued to an electronic storage device (DTD, SDS, SKL or TKL) that has been encrypted with a TRKEK or where the device is either stored separately from its associated CIK or both are controlled, handled and stored under TPI procedures. The devices and associated CIKS will be reflected on the shift/watch-to-watch inventory and properly accounted for at all times.

b. For legacy devices in use (KYK-13 or KYX-15A), the devices will be reflected on local inventories and safeguarded based on the highest classification of key stored in the device.

c. Inventory of tape key is required in accordance with Chapter 7 of this manual.

d. Electronic key generated from/stored on the LMD/KP will be verified by the EKMS Manager/Alternate during account inventories.

1182. ACCOUNTABILITY AND REPORTING REQUIREMENTS:

a. There is no requirement to report field generated electronic key to the COR.

b. Commands converting tape key to electronic form are not required to report distribution of this key to an authorized holder.

c. Distribution of key to an unauthorized holder must be authorized by the CONAUTH of the key. CONAUTHs must ensure that the COR is notified of key distributed to other than an authorized holder. This action is necessary to ensure that all holders are notified in the event that emergency supersession of a key is required.

d. Except for recipients of key received via OTAR, all commands that generate, transmit, relay, or receive electronic key are required to maintain local accounting records.

NOTE: Sending stations that distribute TEK for circuits supported via HTHKT or OTAR must maintain appropriate logs.

(1) **OTAD/OTAR/OTAT Logs**: Commands that generate, transmit, receive and relay electronic key for OTAD/OTAR/OTAT must retain local accounting records in accordance with Annex T. The retention of local records applies to both field-generated key and key converted from tape key.

NOTE: Key tape converted to electronic form for transmission via OTAR/OTAT must be accounted for based on its assigned AL Code. See 1182.d above for OTAR exception related to log requirements.

e. Copies of local accounting records for a generating station (OTAR/OTAT) and relaying/receiving stations (OTAT) are included in Annex Q and R, respectively. Commands will fill in appropriate columns of the accounting records based on the action taken.

f. Record keeping/accounting requirements matrix:

OTAT		**OTAR**	
FLD GEN KEY	**TAPE KEY**	**FLD GEN KEY**	**TAPE KEY**
GL RL	**GC RL**	**GL RN**	**GC RN**

LEGEND: FLD GEN KEY: Field-generated keying material

GC: Key generating station must account for tape key to NCMS in accordance with its assigned AL code. After conversion to electronic form for OTAR/OTAT, "GL" applies. Fill in all columns on the generating station log.

GL: Key generating station must account for key locally. Fill in all columns on the generating station log.

RL: Receiving or relay stations must account for key locally. Fill in applicable columns on the "Receiving/Relay" log.

RN: No accounting is required for recipients.

g. Incomplete Local Accounting Records/Logs:

Failure to properly maintain local accounting records/logs as detailed in this article is a non-reportable Practice Dangerous to Security (PDS). Document locally in accordance with local command directives.

1183. REPORTING OF COMSEC INCIDENTS FOR ELECTRONIC KEY:

a. Use of an unauthorized procedure under **COMSEC emergencies**, as determined by CO/on-scene commander, is not a reportable incident.

b. Detailed guidance for the reporting of COMSEC incidents and PDSs are contained in Chapters 9 and 10, respectively.

1184. NAG 16 (series):

Commands must refer to NAG-16 for detailed information on the following:

a. Specific OTAR/OTAT communications procedures (e.g., KW-46).

b. Allied OTAR doctrine.

c. Use of ICP Generic Key as OTAR/OTAT KEK.

d. Procedures for distributing key via DSN/GENSER message system, STE, TRI-TAC, and MSE.

e. Unsuccessful OTAR situations.

f. Late joiners to nets.

g. Key tape ordering guidance.

h. List of all 128-bit crypto-equipment.

i. Procedures for transferring key and tag from one DTD (AN/CYZ-10) to another via STE.

1185. KP SPECIFIC ISSUES:

a. **General**: The unkeyed KP is SECRET, AL Code 1 because as a key generator/processor handling bulk keying material, it is much more sensitive than normal COMSEC equipment. The KP is approved for use up to TOP SECRET, if privileged, including processing key of all classifications and categories. The KP is normally SECRET, but becomes TOP SECRET when outputting unencrypted TOP SECRET key.

b. **Keying**: There are two types of keys handled by the KP:

(1) Keys needed for the KPs own internal use (KP keys).

(2) Keys handled (e.g., generated, encrypted, decrypted, stored, issued) by the KP for use in other cryptographic devices, equipment, or systems.

c. **KP CIKS**: All KP CIKs (e.g., Transit CIKs, System Administrator CIKs, User CIKs) are classified SECRET. They may be declassified once they are disassociated/deleted from the KP. The Transit CIK is AL Code 4 with all other CIKs being locally accountable with no AL Code assigned.

d. **REINIT 1 AND NAVREINIT 2 KEYS**: These are **NOT KP "CIKs"** they are "build fields" used to create internal keys. REINIT 1 and NAVREINIT 2 are **not** used to generate or output TOP SECRET key. They are used **only** when it is necessary to reinitialize a new KP (e.g., the command's current KP is due for recertification or new replacement KP).

(1) REINIT 1 and NAVREINIT 2 are classified SECRET or TOP SECRET to reflect the command’s HCI/privileges. They are not designated Crypto and do not require TPI storage or handling.

(2) REINIT 1 keys are AL Code 1 COMSEC accountable to minimize their mishandling (i.e., premature zeroization) and physical loss. REINIT 1 keys must be accounted for as ALC 1 material as described below.

(3) LCMS provides the EKMS Manager with the ability to create backup copies of REINIT copies. All EKMS accounts **will** make four (4) copies of REINIT 1 and two (2) copies of NAVREINIT 2 and account for these keys as outlined below. EKMS accounts must make these copies and report them to NCMS per the following guidance:

(a) REINIT 1 keys will be brought into COMSEC Material Control System ***and*** LCMS accountability as a “COMSEC **Aides**” (Material Type) using a *Reportable* SF-153 Possession Report. This report must be submitted to the COR for processing.

(b) NAVREINIT 2 keys will be brought into LCMS accountability as “Equipment” (Material Type) using a *Local* - SF-153 Possession Report. This report will not be submitted to the COR.

NOTE: Retention requirements for SF-153 Possession Reports are reflected in Annex T.

(c) The REINIT keys will be physically tagged using the registration data described in this article.

(d) Procedures for registering/entering the new short titles into COMSEC accountability/LCMS follow:

1. **Short titles for REINIT Keys:** The short title for REINIT 1 keys is REINIT 1 (there is a space between REINIT and the number 1). The short title for NAVREINIT 2 keys is NAVREINIT 2 (there is a space between NAVREINIT and the number 2).

2. **Edition:** For REINIT 1 keys, the date that the REINIT key was created will serve as the edition.

Format the date in this manner: YYMMDD. NAVREINIT 2 keys are not assigned an edition.

3. **Register number:** REINIT 1 keys are assigned a register number. This is the engraved numerical portion of the serial number on the KSD-64A (usually 4 digits). The preceding alpha character will not be used. NAVREINIT 2 keys are not assigned register numbers because they are accountable by quantity per AL Code 4 rules.

4. Examples of properly registered REINIT 1 keys follow immediately:

Short title:	**Edition:**	**QTY:**	**REG #:**	**AL Code:**
REINIT 1	030503	1	4682	1
REINIT 1	040203	1	5399	1

5. Examples of properly registered NAVREINIT 2 keys follow immediately:

Short title:	**Edition:**	**QTY:**	**REG #:**	**AL Code:**
NAVREINIT 2	Not assigned	1	Not assigned	4
NAVREINIT 2	Not assigned	1	Not assigned	4

6. When entering this information into LCMS, EKMS Managers may see the following LCMS pop-up screens: ***Message [08315] A numeric edition has been entered for aides*** (If this message appears, acknowledge it by clicking on acknowledge and continue processing.)

Message [08315] A numeric edition has been entered for non-modern material. Select continue to proceed with preparing the receipt. Select cancel to modify the material type and/or edition. (If this message appears, click continue.)

(4) Disposition of REINIT keys:

(a) REINIT 1 keys must not be zeroized without specific authorization from NCMS. REINIT 1 keys may be zeroized only after a Site Initialization and a system backup are successfully performed in conjunction with an account rebuild and destruction authorization is received. Destruction of REINIT 1 keys must be reported to Tier 1.

(b) Old NAVREINIT 2 keys will be zeroized per this guidance: Changeover requires the use of the NAVREINIT 2 key and two blank KSD-64As. The Changeover process produces two new NAVREINIT 2 keys. After performing a changeover and creating the new NAVREINIT 2 keys, **run a system backup** then zeroize the old NAVREINIT 2 keys via the KP or a three times in a STU-III terminal, if a terminal is still held by the account.

(c) Zeroized REINIT or NAVREINIT KSD-64As may be re-used as necessary for the creation of new REINIT keys.

(5) Accountability and control of REINIT keys will be subject to review during COMSEC Inspections and inventories.

e. **Certification:**

Operational KPs will be recertified on a regular basis or whenever they are repaired, but not less than once every three years. Records will be kept by CMIO Norfolk VA//35// to indicate the date of last certification. CMIO Norfolk will ship a replacement KP 60 days prior to recertification date. Accounts will be notified by message when shipment is entered into DCS. The internal KP battery should last throughout the recertification period. If the KP low battery light illuminates, contact NCMS WASHINGTON DC//N34// immediately for a replacement. Until the battery is replaced, the KP should remain plugged into an AC power source to prevent automatic zeroization. After the replacement KP is received and is operational, zeroize the replaced KP and send the unit to CMIO Norfolk VA Broken Copy Stock, ACCOUNT 078202 for recertification, which includes battery replacement.

(1) EKMS managers must zeroize the KP prior to shipment. If the KP cannot be zeroized, the SF-153 must be annotated with the reason why.

(2) The only method approved for shipping KPs is via DCS courier.

AMD-9

(3) There is no recertification requirement for TESTPACs held by the EKMS School Houses or ~~CMS AA Training~~ COR Audit Teams.

f. **Reporting Zeroized KOK-22s/KPs**:

Several Navy commands have reported receiving KPs in a zeroized state (i.e., without the internal key that facilitates site initialization and other functions). Fluctuations in and temporary cessations of electrical power, such as when initially connecting the KP to a power source or when temporarily disconnecting and reconnecting the KP from one power source to another, have also caused zeroizations. Until such time as these unwanted zeroizations can be eliminated, the following guidance applies:

(1) All such zeroizations must be reported by message and addressed as follows:

ACTION: NCMS WASHINGTON DC//N3/N34/N5//
The respective COR (DIR TIER1 SAN ANTONIO TX
or CSLA TIER1)
INFO: CMIO NORFOLK VA//35///
COMSPARWARSYSCOM//PMW 161//
SPAWARSYSCEN ATLANTIC CHARLESTON SC
//752/721SR/752PR/752RL//
DIRNSA FT GEORGE G MEADE MD//I31132//
ADMIN CHAIN OF COMMAND OR
OPERATIONAL CHAIN OF COMMAND (AS APPROPRIATE)
SERVICING A&A TEAM

SUBJ: KP ZEROIZATION

(2) The message must describe the cause (if known) or circumstances surrounding zeroization as well as request disposition instructions for zeroized KP. Advise if a spare KP is available to use while primary KP is inoperable.

(3) Commands must not take any additional steps to further zeroize the KP in preparation for shipment/return to manufacturer or depot. Doing so will interfere with the manufacturer’s ability to determine the cause for the unwanted zeroization.

(4) Report KP zeroizations as COMSEC incidents only when they are either suspected or known to have occurred from tampering or other malicious activity. See Article 945.e.(12)(e). Address any questions on reporting requirements to your servicing ~~CMS A&A~~ COR Audit Team or NCMS (N5 or N7).

AMD-9

g. **Emergency Protection**:

Follow the provisions of Annex M for the emergency protection of materials in this document. To destroy the KP beyond reuse during emergencies (e.g., impending site overrun and capture), where the alternative is possible compromise of the KP and the key/data it protects, zeroize the KP and, if time allows, using a Torx-15 bit remove the motherboard and destroy it by incineration. If time does not allow for removal of the motherboard, zeroize the KP and use thermite grenades to melt the box down through to the motherboard.

ANNEX A

GLOSSARY

Access: The opportunity and capability to obtain knowledge of COMSEC material, or to use, copy, remove, or tamper with it. A person does not have access merely by being in a place where COMSEC material is kept, as long as security measures (e.g., physical, technical, or procedural) prevents them from having an opportunity to obtain knowledge of, or alter, information or material.

Access Control List (ACL): ACL is a customized list of remote users that are allowed to establish a secure session with the terminal containing the ACL. This list can be comprised exclusively of unique Keying Material Identifiers (KMID) or generic Department Agency Organization (DAO) codes or a mixture of both KMID and DAO codes.

Account Clerk: An individual assigned to assist EKMS account personnel in the execution of certain administrative duties associated with the management of a EKMS account. Clerks may not be registered and granted access to the LMD/KP and appointment of an Account Clerk is at the discretion of the Commanding Officer.

Account registration: Process by which EKMS entities are identified and associated with their administrative and configuration attributes.

Accountable Items (A/I) Summary: A list of all COMSEC material held in an EKMS numbered CMS account.

Accounting Legend (AL) Code: A numeric code used in the COMSEC Material Control System (CMCS) to indicate the minimum accounting controls required for an item of accountable COMSEC material. The AL Code is not a classification marking.

Accounting number: Also referred to as either a "reg or serial number" is assigned to an individual item of COMSEC material for accountability purposes.

AMD-9

~~Advice and Assistance (A&A) Training~~ COR Audit Team: Worldwide network of CMS subject matter experts who provide training and assistance to personnel with COMSEC responsibilities and conduct EKMS/KMI Audits.

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

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

AL Code 4: AL Code 4 COMSEC material is locally accountable by quantity after initial receipt.

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

AL Code 7: AL Code 7 COMSEC material that is electronically generated and is locally accountable to the generating facility. All key transfers, including all subsequent transfers, must also be reported to the generating facility.

Alternate EKMS Manager: Individual(s) designated to assist the primary EKMS Manager in the performance of his/her duties and to perform Manager duties during the temporary absence of the EKMS Manager.

> **NOTE: Alternate Managers share equally the responsibilities for proper account management with the EKMS Manager.**

Amendment: A correction or change to a COMSEC publication.

Appointment Letter: Used by COs to formally designate the assignment of custodian personnel and CMS Clerks/Accountants.

Archive: To file or store records off-line.

Assembly: A group of parts, elements, subassemblies, or circuits that are removable items of COMSEC equipment.

Association: This is the initial cryptographic binding between a KSV-21 card and a STE where a component of the Crypto-Ignition Key (CIK) is transferred from the card to the STE.

Audit: Independent review and examination of system records and activities to assess the adequacy and effectiveness of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Audit Data: Contents of one or more audit records.

Audit Trail: Chronological record of system activities that enable the reconstruction and examination of the sequence of events and/or changes in an event.

Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's eligibility to receive specific categories of information.

Authentication Information: Unclassified information which identifies a STE terminal. Authentication information is specified for each STE key ordered and is included as part of the key. Each terminal’s authentication information is displayed on the distant terminal during a secure call.

Authenticator: Means used to confirm the identity or eligibility of a station, originator, or individual.

Auto-manual system: Programmable, hand-held device used to perform encoding and decoding functions.

Automated Information System (AIS): Any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data and includes computer hardware, firmware, and software.

> **NOTE: Included are computers, word processing systems, networks, or other electronic information handling systems, and associated equipment.**

Automatic remote Rekeying (AK): Procedure to rekey a distant crypto-equipment electronically without specific actions by the receiving terminal operator.

Benign: Condition of cryptographic data such that it cannot be compromised by human access to the data.

> **NOTE: The term benign may be used to modify a variety of COMSEC-related terms (e.g., key, data, storage, fill, and key distribution techniques.**

Binding: Process of associating a specific communications terminal with a specific cryptographic key or associating two related elements of information.

BLACK: Designation applied to telecommunications and automated information systems, and to associated areas, circuits, components, and equipment in which only unclassified signals are processed. **[NOTE: Encrypted signals are unclassified.]**

Black bulk facility: A telecommunications facility that employs crypto-equipment to protect multichannel trunks passing encrypted or unclassified information.

BLACK key: Encrypted key.

Broadcast Area Variable (key) (BAV): This key is used in conjunction with two other keys (e.g., the Community Key (CV) and Unique Key (UV), for KW-46 secured broadcasts). Navy uses four separate BAVs for its broadcasts covering the Western Pacific/Indian Ocean, Eastern Pacific, Atlantic and Mediterranean areas.

Bulk encryption: Simultaneous encryption of all channels of a multichannel telecommunications trunk.

Call sign cipher: Cryptosystems used to encipher/decipher call signs, address groups, and address indicating groups.

Canister: Type of protective package used to contain and dispense key in punched or printed tape form.

Carry Card: The CIK component stored in a STE can be transferred to a KSV-21 card not associated with the STE. Once the component is transferred, this card is now known as a carry card and it is used to establish multiple STE associations with a single user card

Central Office of Record (COR): A central office which keeps records of all accountable COMSEC material held by elements subject to its oversight.

Chief of Naval Operations (CNO): CNO (N614), Head, Navy Information Security (INFOSEC) Branch, has overall authority for Naval Telecommunications to include COMSEC policy. The CNO is the COMSEC resource sponsor for the DON.

Chronological File: Used to maintain COMSEC material accounting reports, A/I Summary pages, inventory reports, transaction logs, CMS Form 1 and/or USTRANSCOM Form 10, and SD Form 572.

COMLANTFLT/COMPACFLT/COMUSNAVEURINST C2282.1 (series): Basic Shipboard Allowance of COMSEC Material. This instruction provides basic CMS account requirements for Atlantic/Pacific surface and subsurface units by hull type and ocean area.

CJCSI 3260.01 (series): Joint Policies and Procedures Governing Positive Control Material and Devices.

Class 6 Code: A two-digit code corresponding to a specific Class 6 field in the identification data displayed on the STE terminal. A Class 6 code is entered on the Key Ordering Authorization Form for users who require additional authentication information (e.g.; security caveats).

Closing Action Authority (CAA): Administrative senior or other designated command that reviews details of incidents or insecurities reported by their subordinate commands.

CMS 25: Single-copy segmented COMSEC keying material destruction report.

CMS 25B: Bi-monthly single-copy segmented COMSEC keying material destruction report.

CMS 25MC: Multiple-copy segmented COMSEC keying material destruction report.

CMS Form 1: Locally prepared form used to authorize appropriately cleared personnel to receipt for and courier COMSEC material between their command and CMIO.

Code: System of communications in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length. Codes may or may not provide security. Common uses include: (a) converting information into a form suitable for communications or encryption, (b) reducing the length of time required to transmit information, (c) describing the instructions which control the operation of a computer, and (d) converting plain text to meaningless combinations of letters or numbers and vice versa].

Code book: Book or other document containing plain text and code equivalents in a systematic arrangement, or a technique of machine encryption using a word substitution technique.

Cold start: Procedure for initially keying crypto-equipment.

COMDTINST M5500.23 (series): Coast Guard Classified Information Management Manual. Provides regulations and guidance for Department of Transportation and Coast Guard units/personnel for classifying and safeguarding classified information and the protection of Coast Guard assets and personnel.

Command Authority (CMDAUTH): Individual responsible for the appointment of user representatives for a department, agency, or organization and assignment of their key ordering privileges.

Commandant, Marine Corps (CMC): CMC Command, Control, Communications, and Computers (C4) Department serves as COMSEC resource sponsor for the Marine Corps. The C4 Department coordinates with CNO, COMNAVIDFOR, and NCMS to establish, promulgate, and oversee EKMS account management matters unique to the Marine Corps. The C4 Department is the focal point for requirements and administration for all Marine Corps EKMS accounts.

Commander, U.S. Coast Guard C4IT Service Center Information Assurance Branch (C4ITSC-BOD-IAB): Acts as the USCG Service Authority (SA) and exercises overall authority for USCG COMSEC matters and also serves as the USCG Program Manager and Principal Agent for the USCG COMSEC Program and also functions as the USCG; **Service Authority, Closing Action Authority, Command Authority (CA) and USCG ISIC.**

Commander, Navy Information Dominance Forces (COMNAVIDFOR): Implements the DON CMS/EKMS program.

Commanding Officer (CO): Individual ultimately responsible for the proper administration of his/her command's EKMS account and compliance with established CMS policy and procedures. An OIC and SCMSRO have the same responsibilities as a CO.

Communications Security (COMSEC): Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government concerning national security, and to ensure the authenticity of such telecommunications. COMSEC includes cryptosecurity, emission security, transmission security, and physical security of COMSEC material and COMSEC information.

Community Variable (key) (CV): This key is used in conjunction with two other keys, the Broadcast Area Variable (BAV) and Unique Key (UV), for KW-46 for secured broadcasts. Separate tape CVs are used for Navy surface ship general service (GENSER) and submarine GENSER fleet broadcasts, the U.S. Navy Special Intelligence (SI) broadcasts, the U.S. Coast Guard broadcasts, and the NATO broadcasts. CVs may also be generated by certified KG-83/KGX-93/93A key variable generators and distributed electronically via OTAR or OTAT.

Compromise: Disclosure of information or data to unauthorized person(s), or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

Compromised Key List (CKL): A list of compromised STE keying material distributed by the EKMS CF during rekey calls.

Computer Security (COMPUSEC): Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer.

COMSEC aid: COMSEC material, other than an equipment or device, that assists in securing telecommunications and which is required in the production, operation, or maintenance of COMSEC systems and their components. **Examples include but is not limited to; call signs/frequency systems, and operating and maintenance (KAO/KAMS) manuals.**

COMSEC emergency: Operational situation, as perceived by the responsible Commanding Officer/on-scene commander, in which the alternative to strict compliance with procedural restrictions affecting use of a COMSEC equipment would be plain text communications.

COMSEC equipment: Equipment designed to provide security to telecommunications by encrypting data for transmission and decrypting data for authorized recipients; also, equipment designed specifically to aid in, or as an essential element of, the conversion process.

> **NOTE: COMSEC equipment includes crypto, crypto-ancillary, crypto-production, and authentication equipment.**

COMSEC facility: Space employed primarily for the purpose of generating, storing, repairing, or using COMSEC material.

COMSEC Incident: Any uninvestigated or unevaluated occurrence that has the potential to jeopardize the security of COMSEC material or the secure transmission of classified or sensitive government information; OR any investigated or evaluated occurrence that has been determined as not jeopardizing the security of COMSEC material or the secure transmission of classified or sensitive government information. COMSEC incidents and insecurities are categorized as cryptographic, personnel, or physical.

COMSEC Incident Monitoring Activity (CIMA): The office within a department or agency that keeps a record of COMSEC incidents and insecurities caused by elements of that department or agency, and ensures that all actions required of those elements are completed. **NCMS is the CIMA for the DON.**

COMSEC insecurity: A COMSEC incident that has been investigated, evaluated, and determined to have jeopardized the security of COMSEC material or the secure transmission of classified or sensitive government information.

COMSEC Material: Items designed to secure or authenticate telecommunications. COMSEC material includes but is not limited to key, equipment, devices, documents, firmware or software that embodies or describes cryptographic logic or other items that perform COMSEC functions.

COMSEC Material Control System (CMCS): A logistics and accounting system consisting of all COMSEC CORS, cryptologic depots and EKMS accounts through which COMSEC material is distributed, controlled, and safeguarded.

COMSEC Material Issuing Office (CMIO): A member of the Vault, Depot Logistics System (VDLS). It is the DON distribution point for COMSEC equipment, publications/manuals and related devices. CMIO is the PMHS for Navy in the EKMS.

Contingency key: Key held for use under specific operational conditions or in support of specific contingency plans. Such material is reflected as “WHENDI” on the SCMR.

Controlled Cryptographic Item (CCI): A secure telecommunications or information handling equipment, or associated cryptographic component that is unclassified but governed by a special set of control requirements. Such items are marked "CONTROLLED CRYPTOGRAPHIC ITEM" or, where space is limited, "CCI".

Controlling Authority (CONAUTH): Designated official responsible for directing the operation of a circuit/cryptonet and for managing the operational use and control of keying material assigned to a circuit/cryptonet. The CONAUTH for field-generated electronic key is the Commander who directed generation of the key. Electronic key converted from key tape remains under the purview of the paper key's designated CONAUTH.

COR Accounting Reports: Documents (SF-153s or COR-generated reports) used by account personnel to document and report to the COR the receipt, transfer, inventory, destruction or other disposition of COMSEC materials. Some examples include: COR-generated Inventory Reports, SF-153 Relief from Accountability Possession, Destruction, Transfer and Receipt reports.

Correspondence and Message File: Used to maintain EKMS account establishment correspondence, EKMS Manager and Clerk appointment correspondence, COMSEC incident and PDS reports, correspondence relating to command allowance and authorization to store classified COMSEC material, and ~~CMS Assist Visit and Inspection~~ audit correspondence.

AMD-9

CRYPTO: A marking or designator identifying COMSEC keying material used to secure or authenticate telecommunications carrying classified or sensitive U.S. government or U.S. government-derived information and is not a security classification. When written in all upper case letters, CRYPTO has the meaning stated above. When written in lower case as a prefix, crypto and crypt are abbreviations for cryptographic. The caveat CRYPTO is applied only to key used on-the-air.

Crypto-ancillary equipment: Equipment designed specifically to facilitate efficient or reliable operation of crypto-equipment, but that does not perform cryptographic functions.

Crypto-equipment: Equipment that embodies a cryptographic logic.

Cryptographic: Pertaining to or connected with cryptography.

Cryptographic component: The hardware or firmware embodiment of the cryptographic logic in a secure telecommunications or automated information processing system. A cryptographic component may be a modular assembly, a printed wiring assembly (PWA), a microcircuit, or a combination of these items.

Cryptographic High Value Products (CHVPs): NSA-approved products incorporating only UNCLASSIFIED components and UNCLASSIFIED cryptographic algorithms. This does include commercial off-the-shelf (COTS) products approved by NSA, but does not include composed commercial solutions or their components, unless an individual component has been approved as a CHVP. Unkeyed CHVPs are not classified or designated as Controlled Cryptographic Items (CCIs). Examples of CHVPs include the IPS-250 and the RF-310M-HH.

Cryptographic incident: Any uninvestigated or unevaluated equipment malfunction, or operator or custodian error that has the potential to jeopardize the cryptosecurity of a machine, auto-manual or manual cryptosystem OR any investigated or evaluated occurrence that has been determined as not jeopardizing the cryptosecurity of a machine, auto-manual, or manual cryptosystem.

Cryptographic information: Crypto keying material and authenticators that are classified TOP SECRET or SECRET and designated as CRYPTO and includes all cryptographic media that embody, describe or implement classified cryptographic logic, to include, but not limited to, full maintenance manuals, cryptographic descriptions, drawings of cryptographic logic, specifications describing a cryptographic logic, and cryptographic software, firmware, or repositories of such software as magnetic media or optical disks.

Cryptographic insecurity: A crypto incident that has been investigated or evaluated and determined to have jeopardized the cryptosecurity of a machine, auto-manual, or manual cryptosystem.

Cryptography: Principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.

Crypto-Ignition Key (CIK): Device or electronic key used enable secure operations of crypto-equipment.

Cryptonet: Three or more elements that use, in common, a short title of keying material.

Cryptoperiod: Time span during which each key setting (i.e., key segment or key card) remains in effect.

Cryptosecurity: Components of communications security that result from the provision of technically sound cryptosystems and their proper use.

Cryptosystem: Associated COMSEC items interacting to provide a single means of encryption or decryption.

Department Agency Organization code (DAO): An identification (six-digit) number associated with a DAO description. This number is assigned by the CF. and is used by the User Representative when placing a keying material order.

Data Encryption Standard (DES): Cryptographic algorithm designed for the protection of unclassified information and published by the National Institute of Standards and Technology in Federal Information Processing Standard (FIPS) Publication 46.

Data transfer device (DTD): A fill device used to store and distribute electronic key which also records activities and provides the ability to review audit trail data related to all key actions/transactions (e.g., issues, zeroization, transfers, etc.) Devices such as the Secure Data Transfer Device 2000 (SDS) and Simple Key Loader (SKL) are also referred to in National Policy as next-generation Data Transfer Devices.

DCS Manual 5200.1 (series): Details administrative and operational procedures for the Defense Courier Service (DCS).

Defense Courier Service (DCS): A joint command of the DOD. The DCS provides the principal means for the secure and rapid transportation of DOD and other qualified material requiring controlled handling by courier authorized customers.

Designated Approving Authority (DAA): Entity designated to ensure coordination and approval of security certification and accreditation for each Navy Tier 2 facility and operation. (NCMS is designated as DAA for Navy Tier 2 facilities and operations).

Directives File: Contains a copy of each effective directive of the command and higher authority that relates to CMS matters (e.g., guidance for local elements/User personnel, letters of Agreement (LOA), and waivers of COMSEC policy and procedures).

Defense Courier Service (DCS): Courier service for the transport of classified material and some unclassified material when certain conditions apply. Accounts that require DCS must contact DCS to obtain a DCS account/address.

EKMS 1 (series): Policy and Procedures for Navy Electronic Key Management System.

EKMS 2 (series): CMS Advice and Assistance (A&A) Training Team Procedures.

EKMS 3 (series): CMS Inspection Manual.

EKMS 5 (series): CMS Cryptographic Equipment Information/Guidance Manual

EKMS 704: The Local Management Device/Key Processor Operator's Manual.

EKMS Account: An administrative entity, identified by a six-digit account number, responsible for maintaining accountability, custody and control of COMSEC material. Also identified as or referred to as a COMSEC account.

EKMS CF: The part of Electronic Key Management System (EKMS) Central Facility (CF) that provides accounting support to NCMS, the Navy's Central Office of Record (COR), and to Navy COMSEC Managers.

EKMS Intelligent Computer Assisted Trainer (ICAT): Computer-based software training program embedded in the LCMS program. Also known as the LCMS CBT.

EKMS Manager: An individual designated by his/her Commanding Officer or other proper authority to be responsible for all actions associated with the receipt, handling, issue, safeguarding, accounting, and disposition of COMSEC material/equipment assigned to a command's EKMS numbered account.

Electronic key: Encrypted or unencrypted key in electronic form that is stored on magnetic media or in electronic memory, transferred by electronic circuitry, or loaded into COMSEC equipment.

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, storing, filling, using, and destroying of electronic key and management of other types of COMSEC material.

Electronically generated key: Key produced only in non-physical form.

> **NOTE: Electronically generated key stored magnetically (e.g., on a floppy disk) is not considered hard copy key.**

Element: Removable item of COMSEC equipment, assembly, or subassembly which normally consists of a single piece or group of replaceable parts.

Embedded cryptography: Cryptography that is engineered into an equipment or system, the basic function of which is not cryptographic.

> **NOTE: Components comprising the cryptographic module are inside the equipment or system and share host device power and housing. The cryptographic function may be dispersed or identifiable as a separate module within the host.**

Emergency modification of holdings: An unforeseen and urgent operational requirement, as determined by the Commanding Officer, which requires the immediate transfer of COMSEC material.

End-item accounting: Accounting for all of the accountable components of COMSEC equipment by a single short title.

Evaluating authority: The official responsible for evaluating a reported COMSEC incident for the possibility of compromise.

> **NOTE: In the case of COMSEC incidents involving keying material, the evaluating authority may or may not be the material's Controlling Authority.**

Exercise key: Key intended for protection of on-the-air transmissions associated with field training or exercises.

External Local Element: Individuals who require COMSEC support from an EKMS numbered account, or from another Local Element (Issuing), and whose CO is different from the CO of the parent account or servicing Local Element (Issuing). See Annex L for the requirement for a Letter/Memorandum of agreement (LOA/MOA) between such commands.

Extractable keying material: Keying material designed to permit physical extraction and removal of individual segments.

Extraction resistance: The capability of crypto-equipment to resist efforts to extract loaded cryptovariables or key.

Fill Card: A KSV-21 card programmed with keying material and a complete CIK. The card has not yet been associated with a STE.

Fill device (FD): Any one of a family of devices developed to read in, transfer, or store key. Current fill devices are KSD-64A, KOI-18, KYK-13, KYX-15, and DTD.

FIREFLY: Key management protocol based on public key cryptography.

Firefly Credentials: FIREFLY exchange information required by another element/entity in order for both elements/entities to cooperatively generate the same session key.

> **NOTE: Credentials are not considered key and therefore do not have a cryptoperiod. Credentials do have an expiration date which is one month from the first use of a credential or the end of the associated FIREFLY's cryptoperiod, whichever comes first.**

Fixed COMSEC facility: A COMSEC facility that contains classified COMSEC material that is located in an immovable structure or aboard a ship.

Formal Cryptographic Access Program: A program that ensures individuals being granted access to cryptographic material have a proper security clearance, a need-to-know, are briefed/indoctrinated, are authorized in writing by the CO/OIC, is a U.S. Citizen, and signs a SD Form 572.

Full maintenance: Complete diagnostic repair, modification, and overhaul of information systems security equipment, including repair of defective assemblies by piece part replacement.

General Message File: Contains all effective general messages (e.g., ALCOMs, ALCOMLANT ALFAs, ALCOMPAC Ps) that pertain to COMSEC material or COMSEC policy and procedures.

Generic Key: A term used to identify copies of STE keying material that contain the same DAO code description for a department, agency, or organization but is not user or geographical-area specific.

Hand receipt: A document used to record custody of COMSEC material given to, or received from custodian personnel or a CMS User.

Hard copy: Physical keying material, such as printed key lists, punched or printed tapes, or programmable read-only memories.

Highest Classification Indicator (HCI): Used to determine the highest classification of COMSEC material that an account may hold.

Immediate Superior in Command (ISIC): Command responsible for the administrative oversight of all CMS matters for their subordinate commands.

Insecure Practices: Occurrences, which, although not reportable outside the violating command, have the potential to jeopardize the security of STE COMSEC material if allowed to perpetuate.

Internal Local Element: Individual(s) who require COMSEC support from an EKMS numbered account, or from another Local Element (Issuing), and whose CO is the same as the parent account or servicing Local Element (Issuing).

Inter-service transfer: Transfer of COMSEC material between a DON EKMS account and a COMSEC account of another service, agency, department, nation, or commercial contractor.

Intra-service transfer: Transfer of COMSEC material between two DON EKMS accounts.

Intrusion Detection System (IDS): A system designed to detect and signal the entry of unauthorized persons into a protected area (e.g., security alarms, sensor systems, video systems).

Inventory: A process described through the physical verification or sighting of each item of accountable COMSEC material charged to a EKMS account or maintained on a local custody basis

Irregularly superseded keying material: Keying material that is superseded based on use and not on a pre-determined supersession date.

Joint Theater COMSEC Management Office (JTCMO): Formed by combining COMSEC management facilities (MCMO/TCMO) of two or more services in support of all accounts within a Joint Theater Area of Operation. Performs receipt, processing, and distribution of all COMSEC material for the Joint Commands.

KAM: Cryptographic Maintenance Manual for a cryptosystem.

KAO: Cryptographic Operating Manual for a cryptosystem.

Key: Information (usually a sequence of random binary digits) used initially to set up and periodically change the operations performed in crypto-equipment for the purpose of encrypting/decrypting electronic signals, for determining electronic counter-countermeasures patterns (e.g., frequency hopping or spread spectrum), or for producing other key).

> **NOTE: "Key" has replaced the terms "variable", "keying variable", and "cryptovariable".**

Key Conversion Notice (KCN): An EKMS CF notice that reflects the keying material identification numbers of seed key which has been successfully converted through a successful a conversion call.

Key Encryption Key (KEK): Key that encrypts or decrypts other key for transmission or storage.

Key fill: Process by which key is moved into end equipment.

Key generation: The process by which a key is created.

Key Inventory List or IL: An inventory report produced by the EKMS CF and distributed to EKMS accounts. EKMS CF ILs list only that STE keying material charged to a particular account as of the inventories preprinted date.

Key list: Printed series of key settings for a specific cryptonet.

> **NOTE: Key lists may be produced in list, pad, or printed tape form.**

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.

Key tape: Punched or magnetic tape containing key. When printed in tape form is also referred **to as a key list**.

Key Storage Device (KSD-64A): A physical device that can be used as either a FD or a CIK. It is a small device that physically resembles a key and contains passive memory. When used to store key it is referred to as a FD. When used to protect keying material that has been downloaded into equipment it is referred to as a CIK.

Key Variable Generator (KVG): A modular, rack mountable unit, which, upon demand, generates 128-bit variables to key distribution, centers, fill devices, or other equipment. It can be operated as a stand-alone device or in a rack in conjunction with other compatible equipment. In either case, the KVG generates variables and transfers them to the front or rear panel interface. KG-83 KVGs are used by the Navy and Coast Guard to generate OTAR TEK for use with KG-84A/84C secured nets and circuits. KGX-93/93A KVGs are used by the Marine Corps to generate key for TRI-TAC switches.

Keyed Terminal: A STE terminal that has been loaded with keying material and an associated card has been inserted.

Keying Material (KEYMAT): A type of COMSEC item in physical or electronic form which supplies either encoding means for manual and auto-manual cryptosystems or key for machine cryptosystems.

Key updating: Irreversible cryptographic process for modifying key automatically or manually.

Legacy Accounts: EKMS Tier 2 Accounts are DON EKMS Accounts that have yet to convert to the newest LCMS Release. These accounts consequently have NCMS as COR for their traditional COMSEC holdings and the Electronic Key Management System Central Facility (EKMS CF) for their modern key holdings. Also see **PT1S Accounts.**

Letter of Agreement (LOA): Defines requirements and responsibilities in those instances where a EKMS account command provides COMSEC material to a command having a different CO.

Limited maintenance: COMSEC maintenance restricted to fault isolation, removal, and replacement of plug-in assemblies.

Local Account/Local Account Command (formerly known as Parent Account Command): The term used to identify an account that provides COMSEC support to other commands or elements. More often than not, these commands or elements are organizationally subordinate to the account command and are called Local Elements (Issuing/Using).

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.

Local custody: The acceptance of responsibility for the proper handling, safeguarding, accounting, and disposition of COMSEC material issued by custodian personnel or local elements.

Local Custody Files: Contains all effective signed local custody documents reflecting the issue of COMSEC material.

Local Custody Issue (LCI) Documents: LCMS-generated and locally prepared forms (e.g., SF-153s) used to document the issue and receipt (acceptance of responsibility) for COMSEC/CCI materials identified therein.

Local Element: Individual responsible for maintaining required files and ensuring the proper safeguarding, storage, and usage of COMSEC material issued from an EKMS numbered account or from another Local Element (Issuing). See Internal Local Element for elements located/attached to the same command. See External Local Element for elements who’s CO is different than that of the EKMS numbered account.

Local Management Device (LMD): Component (i.e., a personal computer (PC)) in EKMS which provides automated services for the management of key and other COMSEC material, and an interface by which additional functionality may be incorporated to enhance its local capabilities.

Long title: Descriptive title of a COMSEC item.

Loss of accountability: A condition which exists when material is charged to an account, cannot be accounted for and no Destruction, Relief from Accountability, Transfer report or Local Custody document is on file to ensure a continuous chain of custody exists for the material.

Maintenance key: Key, not marked CRYPTO, which is intended only for off-the-air, in-shop use.

Manual cryptosystem: Cryptosystem in which the cryptographic processes are performed manually without the use of crypto-equipment or auto-manual devices.

Manual remote rekeying (MK): Procedure by which a distant crypto-equipment is rekeyed electronically, with specific actions required by the receiving terminal.

Material Control User (MC User): An individual authorized in writing by the CO/OIC to manage the features and capabilities of a STE for other users, including software upgrades for the STE and KSV-21 cards when necessary. The appointment of MC User is recommended for accounts with a large number of terminals or accounts that have local elements that are geographically distant.

Material User: Individual responsible for the proper security, control, accountability, and disposition of the COMSEC material placed in his/her charge. A material user is known as a Local Element (LE) in the EKMS infrastructure.

> **NOTE: A Material User may or may not have signed for COMSEC material.**

Maximum Security Level (MAXSL): This feature prohibits a remote user from using a higher key classification than the set MAXSL to establish a secure session. Normally this is used to prevent a user from contaminating the system with higher classified information than the certified level of the system.

MEF COMSEC Management Office (MCMO): The ISIC for USMC Marine Expeditionary Forces.

Modern Key: A collective name for FIREFLY-type key either STE Keying material, SDNS Communications Key or SDNS MSK.

Minimize: A condition imposed on users of DOD telecommunications networks where normal message and/or telephone traffic is drastically reduced so that messages connected with an actual or simulated emergency will not be delayed.

Minimum Security Level (MINSL): This feature prohibits a remote user from using a lower key classification than the set MINSL to establish a secure session. Normally this is used to prevent a user not meeting the minimum security level accessing a higher classified information system.

Mobile COMSEC facility: COMSEC facility that can be readily moved from one location to another (e.g., a van).

Mobile User: For COMSEC purposes, a term encompassing Marine Tactical, Naval Special Warfare (SPECWAR), Naval Construction Battalion, Mobile Inshore Undersea Warfare Unit (MIUWU), Explosive Ordnance Disposal (EOD) units, Mobile Self-Contained Command Post (MSQ) units, Mobile Ashore Support Terminal (MAST) units, Mobile Integrated Command Facility Pacific (MICFAC) units, and all aircraft.

> **NOTE: Units identified above are considered mobile users when operating in a tactical/field environment at a temporary site away from their permanent operating base or area.**

Modern key: Refers collectively to the following types of key: Asymmetric, EFF, FF, MSK, SDNS and STE.

Modification: Any NSA-approved mechanical change to the electrical, mechanical, or software characteristics of a COMSEC equipment, assembly, or device.

> **NOTE: Classes of modifications are: mandatory, optional/special mission, and repair action.**

NAG-16 (series): Field Production and Distribution of Electronic Key in Support of Short-Notice Operations.

> **NOTE:** Annex C **contains compromise assessment guidance on evaluating COMSEC incidents involving field-generated electronic key.**

National COMSEC Incident & Reporting Evaluation System (NCIRES): System established by the National Security Agency (NSA) for evaluating incidents involving COMSEC material.

National Security Agency (NSA): Executive agent for developing and implementing national policy for COMSEC material. Produces and develops most COMSEC material used to secure the transmission of classified or sensitive unclassified information.

Naval Communications Security Material System (NCMS): Administers DON CMS program and functions as SERVAUTH for DON EKMS Accounts. Serves as COR/Tier 1 for Legacy Tier 2 Accounts.

NAVICPINST 2300.4 (series): Utilization and Disposal of Excess Communications Security (COMSEC) Material. This instruction provides procedures for utilization, turn-in, and disposal of excess COMSEC material.

Net Control Station (NCS): Terminal in a secure telecommunications net responsible for distributing key in electronic form to the members of the net.

No-lone zone: An area, room, or space to which no one person may have unaccompanied access and which, when occupied, must be occupied by two or more appropriately cleared individuals who remain within sight of each other.

Non-extractable keying material: Keying material designed to remain intact in its original physical form (e.g., non-perforated code books, etc.) throughout its entire effective period.

NSTISSI 7003: Protected Distribution Systems (PDS). **Provides guidance concerning use of wire lines or fiber optics for the electrical or optical transmission of unencrypted classified information.**

Operational key: Key, marked CRYPTO, intended for on-the-air protection of operational information or for the production or secure electrical transmission of key streams.

OPNAVINST 2221.3 (series): Communications Security (COMSEC) Equipment Maintenance and Training. **This instruction provides training requirements for COMSEC equipment installation, maintenance, and repair.**

OPNAVINST 2221.5 (series): Release of COMSEC Material to U.S. Industrial Firms Under Contract to U.S. Navy. **This instruction provides policy and procedures for authorizing release of COMSEC material to industrial firms under contract to USN.**

OPNAVINST C5510.93 (series): Navy/Marine Corps Implementation of National Policy on Control of Compromising Emanations (U). **Promulgates within the DON, the policy and procedures for the**

implementation of the national policy on the control of compromising emanations.

OPNAVINST 5530.14 (series): DON Physical Security and Loss Prevention Manual. **This instruction provides standards for physical security and loss prevention measures to safeguard personnel, property, and material at Navy and Marine Corps shore installations and activities.**

Over-the-Air key Distribution (OTAD): Providing electronic key via over-the-air rekeying (OTAR), over-the-air key transfer (OTAT), or cooperative key generation.

Over-the-Air Transfer (OTAT): Electronically distributing key without changing traffic encryption key (TEK) used on the secured communications path over which the transfer is accomplished.

Over-the-Air Rekeying (OTAR): Changing traffic encryption key (TEK) or transmission security key (TSK) in remote crypto-equipment by sending new key directly to the remote crypto-equipment over the communications path it secures.

Page check: Verification that all pages of a publication or technical manual are present.

Parent Account Command: See Local Account or Local Account Command.

Personnel incident: An unevaluated or uninvestigated incident regarding the capture, attempted recruitment, or known or suspected control by a hostile intelligence entity, or unauthorized absence or defection of an individual having knowledge of or access to COMSEC information or material, that has the potential to jeopardize COMSEC information or material; OR any investigated or evaluated occurrence that has been determined as not jeopardizing COMSEC information or material.

Personnel insecurity: A personnel incident that has been investigated or evaluated and determined to have jeopardized COMSEC information or material.

Physical incident: An unevaluated or uninvestigated incident regarding any loss of control, theft, capture, recovery by salvage, tampering, unauthorized viewing, access, or photographing that has the potential to jeopardize COMSEC material; OR any investigated or evaluated occurrence that has been determined as not jeopardizing COMSEC material.

Physical insecurity: A physical incident that has been evaluated or investigated and determined to have jeopardized COMSEC material.

Physical Material Handling Segment: The COMSEC Material Issuing Office **(CMIO)** receives, stores, and ships Ready for Issue (RFI) equipment and is the Physical Material Handling Segment (PMHS) for Navy in the EKMS.

Physical security: Physical measures designed to safeguard COMSEC material or information from being accessed or intercepted by unauthorized persons.

Positive control material and devices: A generic term referring to Joint Staff positive control material and devices which includes Sealed Authentication System (SAS), Permissive Action Link (PAL), Coded Switch System (CSS), Positive Enable System (PES), and Nuclear Certified Computer Data (NCCD). NCMS's role for positive control material is limited to accounting functions only.

Precautionary use: The use of keying material, which has possibly been compromised, to support military operations after the Controlling Authority has determined that emergency supersession of the questionable keying material may not be practical.

Primary Tier 1 Segment (PT1S): The layer of EKMS which, at EKMS FOC, will function as the intermediate key generation and distribution center, Central Office of Record, Privilege Certificate Manager, and Registration Authority for EKMS Tier 2 accounts. There are currently two PT1Ss. One is located at Lackland AFB San Antonio TX and the other at Ft. Huachuca AZ. Also see **Tier 1**, **Servicing Primary Tier 1 Segment**, and **NCMS**.

Primary Tier 1 Segment (PT1S) Accounts: PT1S Accounts are those DON EKMS Tier 2 accounts that have converted to the LMD/KP Phase 4 Release and have as their sole Central Office of Record (COR) a Primary Tier 1 Segment (PT1S). Also see **Legacy Accounts.**

Privilege: Authorization to perform a specific function usually restricted to a limited set of individuals or elements.

Privilege Management: Establishment, enforcement, and maintenance of the authorizations that control access to data and functions within EKMS, and the activities that a Service or agency must perform to ensure that the above are accomplished securely, efficiently, and in a manner that best suits the needs of the service or agency.

Protective packaging: Packaging techniques for COMSEC material which discourage penetration, reveal that a penetration has occurred or was attempted, or inhibit viewing or copying of keying material prior to the time it is exposed for use.

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

Protective technologies: Special tamper-evident features and materials employed for the purpose of detecting tampering and deterring attempts to compromise, modify, penetrate, extract, or substitute information processing equipment and keying material. Protective technologies include, but are not limited to, key tape canisters, end-opening key card packages, holographic bags, seals, screw head coating, and logo tape.

PT1S Accounts: See **Primary Tier 1 Segment (PT1S) Accounts.**

Public key cryptography: Type of cryptography in which the encryption process is publicly available and unprotected, but in which a part of the decryption key is protected so that only a party with knowledge of both parts of the decryption process can decrypt the cipher text. Commonly called non-secret encryption in professional cryptologic circles. FIREFLY is an application of public key cryptography.

RECONCILIATION: Process through which received accountable material is added to the local account’s data base.

RED: Designation applied to telecommunications and automated information systems, plus associated areas, circuits, components, and equipment which, when classified plain text signals are being processed therein, require protection during electrical transmission.

RED key: Unencrypted key.

Registration Authority (RA): EKMS element/entity that is responsible for registering an account and assigning the account an EKMS ID (responsibility usually performed by COR for the account).

Regularly superseded keying material: Keying material that is superseded on a regular, pre-determined date for each edition of material regardless of whether or not the material has been used.

Remote rekeying: Procedure by which a distant cryptoequipment is rekeyed electrically.

Reserve On Board (ROB): A quantity of keying material, not yet effective, held in reserve by an account for use at a later date.

Resident alien: A citizen of a foreign country who is legally residing in the United States on a permanent basis.

> **NOTE: Diplomatic personnel are not considered resident aliens.**

SDIP-293: Instructions for the control and safeguarding of NATO Cryptomaterial (Superseded AMSG-293).

SECNAVINST 5040.7 (series): Naval Command Inspection Program. This instruction assigns responsibility and prescribes procedures for the preparation, conduct, reporting, and follow-up of inspections.

SECNAV M5510.30 (series): DON Personnel Security Program. The basic DON regulations governing the PSP.

SECNAV M5510.36 (series): DON Information Security Program (ISP) Regulation. This instruction provides all DON activities and personnel with regulations and guidance for classifying and safeguarding classified information security.

SECNAVINST 5720.42 (series): Department of the Navy Freedom of Information Act (FOIA) Program. This instruction implements DON policies and procedures for handling FOIA requests and FOUO/unclassified information.

Secure Access Control System (SACS): This system is comprised of three independent features: ACL, MAXSL and MINSL.

Seed key: Initial key used to start an updating or key generation process.

Service Authority (SERVAUTH): Entity within each military service that has been designated to administer its COMSEC program and, in so doing, to perform certain management and oversight functions as described for DON in Chapter 1 of this manual (see Article 120 for DON SERVAUTH, *NCMS*).

Servicing Primary Tier 1 Segment (PT1S): Refers to the specific Tier 1 site having primary COR responsibility for Tier 2 accounts. There are currently two PT1Ss. One is located at Lackland AFB, San Antonio TX and the other is at Ft. Huachuca AZ. At EKMS FOC, all Army, Air Force, and DON Tier 2 accounts will be serviced by one or the other of these PT1Ss.

SF-153: Multi-purpose form used to record COMSEC material transactions (e.g., transfer, destruction, inventories, issues).

Short title: A series of letters and/or numbers (e.g., KG-84, USKAT 2333), used for brevity, and assigned to certain COMSEC materials to facilitate handling, accounting, and control.

Simple Key Loader (SKL): is next generation Data Transfer Device, which is accountable in the CMCS as a Controlled Cryptographic Item (CCI) as ALC 1.

SPCCINST 5511.24 (series): Classified Electronic Communications Security (COMSEC) Material in the Navy Supply System. This instruction provides procedures for the security accounting and inventory management control of classified electronic COMSEC material received and issued by the Navy Supply System.

Staff CMS Responsibility Officer (SCMSRO): An individual (O-4 or above), designated by a flag or general officer in command status (or any officer occupying the billet of a flag or general officer with command status), responsible for the proper administration of routine EKMS account matters.

Start-up KEK: Key encryption key held in common by a group of potential communicating units and used to establish ad hoc tactical nets.

Status: Determines the usability of COMSEC material.

> **NOTE: COMSEC material is always in one of three status conditions: reserve, effective, or superseded.**

Status COMSEC Material Report (SCMR): Classified SECRET NOFORN, produced by the COR and provided to Tier 2 accounts automatically each month via their X.400 mailboxes. Contains list of Controlling Authorities, current amendments to publications and status information.

Storage: Pertains to material which is secured using approved procedures when not actually in use preventing unauthorized access. This can include key stored in encrypted form on the LMD/KP.

Storage Key Encryption Key (SKEK): Key used internally by the DTD to encrypt keys stored in the DTD's key storage database. Where the DTD's key storage database is compartmented, there is a unique SKEK per compartment. The SKEK generated in the DTD has a one-year cryptoperiod.

STE User: An individual or group of individuals (e.g.; a watch section or personnel of a particular office) who use STE terminals and KSV-21s to make secure phone calls, regardless of whether or not they have personally signed for the material on local custody.

Supersession: Scheduled or unscheduled replacement of COMSEC material with a different edition.

> **NOTE: Supersession may be regular, irregular, or on an emergency basis.**

Supervisory CIK: Has all the privileges of the User CIK and, in addition, allows the Supervisory User to perform utility functions such as loading application software and uploading and reviewing audit trails. Also see User CIK.

Supervisory User: Individual designated by CO/OIC to create CIKs, assign serial numbers to them, and to fulfill additional responsibilities for their handling and safeguarding.

Tactical Environment: Geographic area of operation in which actual or simulated combat activity involving mobile land, sea, and/or air forces is occurring.

Tactical Key: Traffic encryption key (TEK), Key Encryption Key (KEK), or Transmission Security Key (TSK) intended to secure information or data that is perishable, has low intelligence value (i.e., low national or international sensitivity), and is classified no higher than Secret.

Tactical Secure Communications: Encrypted communications occurring within a tactical environment or lining tactical forces with their fixed command and support activities.

Telecommunications: Preparation, transmission, communication, or related processing of information (writing, images, sounds or other data) by electrical, electromagnetic, electromechanical, electro-optical or electronic means.

TEMPEST: Short name referring to investigation, study, and control of compromising emanation from telecommunications and AIS equipment.

Terminal Privilege Authorities (TPA): The individuals who are responsible for the configuration of the STE security features and the upgrade of the terminal and card software.

Test key: Key, marked CRYPTO, intended for on-the-air testing of COMSEC equipment or systems.

Theater COMSEC Management Office (TCMO): U.S. Army Major Command COMSEC management office.

Tier 0: Central Facility - NSA's Fort Meade and Finksburg key facilities, which provides centralized key management services for all forms of key.

Tier 1: The layer of EKMS which serves as the intermediate key generation and distribution center, Central Office of Record, Privilege Certificate Manager, and Registration Authority for EKMS Tier 2 accounts.

Tier 2: The layer of EKMS comprised of EKMS accounts that manage key and/or other COMSEC material.

Tier 3: The lowest tier or layer of the EKMS architecture, which includes the DTD and all other means used to transfer key to cryptographic equipment.

Traditional Key: Term used to reference non-FIREFLY based key or Netted FF key that is generated in accordance with established procedures.

Traffic Encryption Key (TEK): Key used to encrypt plain text or to superencrypt previously encrypted text and/or to decrypt cipher text.

Training key: Key, not marked CRYPTO, intended for off-the-air training. Training key is restricted to off-the-air, in-classroom use only.

Transaction Status Log: LCMS records and assigns a sequential number to material transactions. This cumulative list of transaction numbers is known as the Transaction Status Log.

Transaction Number (TN): A number used to maintain continuity of COMSEC material transactions.

Transfer Key Encryption Key (TrKEK): Key used in the DTD to decrypt previously encrypted user key (loaded into the DTD as encrypted key) to enable the DTD to output user key in unencrypted form.

Transmission Security (TRANSEC): Component of communications security that results from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.

Transmission Security Key (TSK): Key that is used in the control of transmission security processes, such as frequency hopping and spread spectrum.

Two-Person Control (TPC): Continuous surveillance and control of positive control material and devices at all times by a minimum of two authorized persons, each capable of detecting incorrect or unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements.

Two-Person Integrity (TPI): A system of handling and storing designed to prevent single-person access to certain COMSEC keying material. TPI requires that at least two persons, authorized access to COMSEC material, be in constant view of each other and the COMSEC material requiring TPI whenever that material is accessed and handled. Each individual must be capable of detecting incorrect or unauthorized security procedures with respect to the task being performed.

TPI storage: TPI storage requires using two approved combination locks (each with a different combination) with no one person authorized access to both combinations. Security containers approved for storage of COMSEC keying material are outlined in Chapter 5.

Unkeyed DTD: DTD, which may or may not contain user key and/or TrKEK and does not have its associated CIK inserted.

Unkeyed STE Terminal: A terminal that is either loaded with keying material and its associated CIK has been removed, or one that contains no keying material.

Unique Variable (key) (UV): This key is used in conjunction with two other keys (e.g., the Broadcast Area Variable (BAV) and Community Variable (CV), for KW-46 secured broadcasts). More specifically, UVs are used to decrypt KW-46 BAVs as they are loaded into each using equipment. A separate UV is assigned to each U.S. Navy and U.S. Coast Guard ship or activity that copies any U.S. Navy KW-46 secured broadcasts.

United States National Distribution Authority (USNDA): The consolidated (Air Force, Army, Navy and NSA) COMSEC distribution facility for keying material.

Updating: Automatic or manual cryptographic process that irreversibly modifies the state of a COMSEC key, equipment, device, or system.

U.S. Controlled Facility: A base or building, access to which is physically controlled by US Citizens, US Government employees, or resident aliens who are authorized US Government employees.

U.S. Controlled Space: A space (e.g.; room or floor) within a facility other than a US-Controlled Facility, access to which is physically controlled by US Citizens, US Government employees (including contractors), or resident aliens who are authorized US Government employees.

User: Individual responsible for the proper security, control, accountability, and disposition of the COMSEC material placed in his/her charge. A material user is known as a Local Element (LE) in the EKMS infrastructure.

> **NOTE: A Material User may or may not have signed for COMSEC material.**

User Card: Any KSV-21 card that has an association with a STE is considered a user card for that STE. A user card can be associated with up to nine STEs.

User CIK: Allows the DTD, SKL or other similar operator to perform all the basic key handling, distribution or operational functions of related devices.

User Key: Key which has been loaded into the DTD for storage and subsequent transfer to other cryptographic devices, equipment, or systems.

User Representative (UR):

(1) Person authorized by an organization to order COMSEC keying material and to interface with the keying system to provide information to key users, ensuring that the correct type of key is ordered.

(2) A person formally designated, by the appropriate Command Authority (CA), to order keying material for STE terminals. The EKMS Manager may also be designated to serve as UR.

Vault Depot and Logistics System (VDLS): Manual and automated systems that operate the vaults and depots that physically receive, store, distribute, and directly handle physical COMSEC material.

Violating command: The command, unit, or activity responsible for a reportable COMSEC incident or insecurity.

When directed (WHENDI): Term used to indicate that COMSEC material is not authorized for use or destruction until notified by the material's Controlling Authority.

EKMS Witness: A properly cleared U.S. Government employee (military or civilian) who assists custodian or user personnel in the proper execution of tasks related to the handling and safeguarding of COMSEC material (e.g., receipt, destruction, inventory, adherence to TPI handling requirements).

Working copy: A legacy term primarily associated with locally generated inventories used to physically sight inventory material when the COR provided inventories. Working copies were and remain more effective in the conduct of an inventory as there should never be a line-out or add-on to a working copy of an inventory generated locally; although they were common on COR provided inventories prior to the transition to Tier-1. Although inventories are no longer provided by the COR and are generated entirely or individually by location from an accounts own LMD, the term still exists and pertains to individually generated destruction and inventory reports. Working copies are used to inventory and destroy material by location which is the most efficient manner. Working copies will only reflect material based on its location in LCMS, i.e. on-hand or issued to Radio, SESS, CIC, etc… Line-outs to locally generated inventories indicate an accounting problem, i.e. proper LCI, transfer or destruction procedures were not used and could reveal either a COMSEC incident or PDS.

Zeroize: To remove or eliminate the key from a crypto-equipment or fill device.

Zeroization of a Card: This process allows a user to delete selective key material stored in a KSV-21 card. To completely zeroize a card, the card must be independently zeroized. This feature is accessible only from an associated STE and with the card privileges option enabled.

ANNEX B

COMMONLY USED ABBREVIATIONS AND ACRONYMS

AMD-9

~~A&A~~	~~Advice and Assistance~~
ACL	Access Control List(s)
ADM	Advanced Development Model
ADP	Automated Data Processing
ADPSO	Automated Data Processing Security Officer
AFEKMS	Air Force Electronic Key Management System
A/I	Accountable Item (Summary)
AIG	Address Indicator Group
AIS	Automated Information System
AK	automatic remote rekeying
AKDC	Automatic Key Distribution Center
AKMS	Army Key Management System
AL	Appointment Letter
ALC/AL Code	Accounting Legend Code
ANDVT	Advanced Narrowband Digital Voice Terminal
ARG	Amphibious Ready Group
ASCII	American standard code for information interchange
AUTODIN	Automatic Digital Network
BAV	Broadcast Area Variable (key)
BG	Battle Group

BET	Bulk Encryption Transaction
C3	Command, Control, and Communications
C3I	Command, Control, Communications, and Intelligence
C4	Command, Control, Communications, and Computers
CA	1. COMSEC account 2. crypto analysis 3. Command Authority
CAA	Closing Action Authority
CAC	codes, authenticators, and call signs
CAD	Collective Address Designator
CCEP	Commercial COMSEC Endorsement Program
CCI	Controlled Cryptographic Item
CCIR	Change of Command Inventory Report
CDP	command distribution precedence
CDR	critical design review
CDT	critical developmental testing
CEEP	Cryptographic Equipment Exchange Program
CEOI	Communications Electronics Operation Instruction
CF	Central Facility
CHVP	Cryptographic High Value Product
CIK	Crypto-Ignition Key
CIM	1. Compromised Information Message 2. Communications Improvement Memorandum
CIMA	COMSEC Incident Monitoring Activity

CITA	COMSEC Incident Trend Analysis
CKEK	Contingency Key Encryption Key
CKG	cooperative key generation
CKL	Compromised Key List
CLMD	COMSEC local management device
CM	configuration management
CMC	Commandant Marine Corps
CMCS	COMSEC Material Control System
CMDAUTH or CA	Command Authority
CMIO	COMSEC Material Issuing Office
CMS	COMSEC Material System
CN/CD	Counternarcotic/Counterdrug
CNO	Chief of Naval Operations
CO	Commanding Officer
COI	1. course of instruction 2. community of interest
COMDT COGARD	Commandant, Coast Guard
COMMARCORSYSCOM	Commander, Marine Corps Systems Command
COMMARFORCOM/PAC/RES	Commander Marine Forces Atlantic/Pacific/Reserve
COMNAVIDFOR	Commander, Navy Information Dominance Forces
COMNAVRESFOR	Commander, Naval Reserve Force
COMPUSEC	computer security
COMSC	Commander, Military Sealift Command

COMSEC	communications security
CONAUTH	Controlling Authority
CONUS	Continental United States
COR	Central Office of Record
COTS	commercial off-the-shelf
CPU	Central Processing Unit
CRF	Crypto Repair Facility
CRYPTO	cryptographic-related
CSO	Command Security Officer
CSP	COMSEC Publication
CSPM	COMSEC Publication Manual
CT1	Common Tier 1
CV	Community Variable (CV)
CVBG	Carrier Battle Group
CY	calendar year
D&A	distribution and allowance
DA	destruction automatic
DAA	Designated Approving Authority
DAO	Defense, Agency, Organization
DBES	disk based encryption system
DCS	1. Defense Courier Service 2. Defense Communications Service
DDN	Defense Data Network
DES	data encryption standard

DIRNSA	Director, National Security Agency
DM	destruction manual
DMR	date material required
DMS	Defense Message System
DON	Department of the Navy
DOS	Disk Operating System
DSN	Defense Switched Network
DT	developmental testing
DTD	Data Transfer Device
DT&E	developmental test and evaluation
DTG	date-time-group
EAM	Emergency Action Message
EAP	Emergency Action Plan
ED	edition
EDM	engineering development model
EFF	Enhanced FIREFLY
EFTO	Encrypted For Transmission Only
EKMS	Electronic Key Management System
EKMS FOC	Electronic Key Management System full operational capability
EKMS ICAT	Electronic Key Management System Intelligent Computer Assisted Trainer
ELINT	Electronic intelligence
ELMACO	Electronics Maintenance Support Company
ELSEC	Electronic security

ENDEX	end exercise
EX	exercise
FC	fixed-cycle
FD	fill device
FF	FIREFLY
FIFO	first-in, first-out
FLSCF	Force Logistics Support Cryptographic Facility
FLTSAT	fleet satellite
FMF	Fleet Marine Force
FNBDT	Future Narrow Band Digital Terminal
FOUO	For Official Use Only
FSTS	Federal Secure Telephone Service
FTS	Federal Telecommunications System
FY	fiscal year
GCCS	Global Command and Control System (WWMCC Replacement)
GENSER	General Service
GPS	Global Positioning System
GSA	General Services Administration
HCI	Highest Classification Indicator
HDR	High data rate
HI	Handling Instructions
HTHKT	Haipe-to-Haipe-Key-Transfer

ICP	Inter-theater COMSEC package
IDS	Intrusion Detection System
IET	Individual Encrypted Transaction
IFF	Identification, Friend or Foe
ILS	integrated logistics support
INFOSEC	Information Security
I/O	Input/Output
IOC	initial operational capability
INFOSEC	Information Systems Security
IR	Infrared
IRST	Inventory Reconciliation Status Transaction
ISDN	Integrated Services Digital Network
ISM	Iridium Secure Module
ISIC	Immediate Superior in Command
ISSA	interservice support agreement
ISSO	Information System Security Officer
ISSM	Information Systems Security Manager
IT	in-transit
JCEOI	Joint-Communication Electronics Operations Instruction
JKMS	Joint Key Management System
JTIDS	Joint Tactical Information Distribution System
KAM	cryptographic maintenance manual
KAO	cryptographic operating manual

KCN	Key Conversion Notice
KDC	key distribution center
KEK	Key Encryption Key
KEYMAT	keying material
KG	key generator
KMC	Key Management Center
KMID	Key Material Identifier
KMS	Key Management System
KP	Key Processor
KPF	key production facility
KPK	key production key
KSD	Key Storage Device
KVG	Key Variable Generator
LAN	Local Area Network
LCI	Local Custody Issue
LCMS	Local COMSEC Management Software
LDR	1. local destruction record 2. low data rate
LE	Local Element
LIFO	last-in, first-out
LMD	Local Management Device
LMM	Limited Maintenance Manual
LOA	Letter of Agreement
LOEP	list of effective pages

LOP	Letter of Promulgation
MARG	Marine Amphibious Ready Group
MATSYM	material symbol
MAXSL	Maximum Security Level
MB	megabyte
MCPDS	Marine Corps Publication Distribution System
MEU	Marine Expeditionary Unit
MIC	microfiche
MINSL	Minimum Security Level
MIUWU	Mobile Inshore Undersea Warfare Unit
MMVG	Mandatory Modification Verification Guide
MOA	1. Memorandum of Agreement 2. Modification of Allowance
MOS	metallic oxide semi-conductor
MOU	Memorandum of Understanding
MSE	mobile subscriber equipment
MSS	Mobile Subscriber System
MTF	1. message text format 2. Medical Treatment Facility
MSK	Message Signature Key
NACSI	National COMSEC Instruction
NACSIM	National COMSEC Information Memorandum
NAVREINIT2	Local Key Encryption Key (KEKL) (stored in a KSD-64A)
NCMS	Naval Communications Security Material

	System
NATO	North Atlantic Treaty Organization
NCCD	nuclear command and control document
NCIRES	National COMSEC Incident & Reporting Evaluation System
NCS	1. National Communications System 2. Net Control Station
NCTAMS	Naval Computer and Telecommunications Area Master Station
NCTS	Naval Computer and Telecommunications Station
NES	Network Encryption System
NESP	Navy Extremely High Frequency (EHF) Satellite Communications Program
NISPOM	National Security Telecommunications and Information Systems
NLT	1. no later than 2. not later than
NLZ	no-lone zone
NOFORN	no foreign nationals
NSA	National Security Agency
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NSTISSD	National Security Telecommunications and Information Systems Security Directive
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NTISSI	National Telecommunications and Information Systems Security Instruction

OIC	Officer-in-Charge
OPAREA	operating area
OPCODE	operations code
OPEVAL	operational evaluation
OPM	Ordering Privilege Manager
OPSEC	Operations security
OSD	Operational Security Doctrine
OTAD	over-the-air key distribution
OTAR	over-the-air rekeying
OTAT	over-the-air key transfer
OTC	1. over-the-counter 2. Officer-in-Tactical Command
PAL	permissive action link
PASEP	passed separately
PC	personal computer
PD	pending destruction
PDS	1. practice dangerous to security 2. protected distribution system
PES	positive enable system
PIN	Personal Identification Number
PLA	Plain Language Address
PM	Privilege Manager
PMHS	Physical Material Handling Segment
PQS	Personnel Qualification Standards
PROM	programmable read-only memory

PSTN	Public Switched Telephone Network
PT1S	Primary Tier 1 Segment (Tier 1 San Antonio TX **or** Tier 1 Ft Huachuca AZ)
PWA	printed wiring assembly
QCCP	quick change card plate
RA	Registration Authority
RACE	rapid automatic cryptographic equipment
RAM	random access memory
RDT&E	research development test and evaluation
REINIT1	Local Key Production Key (KPKL) (stored in a KSD-64A)
RF	radio frequency
RFI	ready for issue
RI	routing indicator
ROB	reserve-on-board
ROM	read-only memory
SA	system administrator
S&G	Sargent & Greenleaf
S/T	short title
SACC	special access control container
SACS	Secure Access Control System
SAIR	Semi-Annual Inventory Report
SAS	sealed authentication system
SATCOM	satellite communications

SBI	special background investigation
SBU	sensitive but unclassified
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCMR	Status COMSEC Material Report
SCMSRO	Staff CMS Responsibility Officer
SDIP	SECAN Doctrine and Information Publication
SDNS	Secure Data Network System
SEPCOR	separate correspondence
SF	standard form
SI	special intelligence
SIGINT	signal intelligence
SIGSEC	signals security
SINCGARS	single channel ground and airborne radio system
SIOP	single integrated operational plan
SKL	Simple Key Loader
SOP	Standard Operating Procedures
SQL	standard query language
SSIC	Standard Subject Identification Code
SSO	Special Security Officer
ST&E	security test and evaluation
STE	Secure Terminal Equipment
T1DSW	Type 1 Disabled Software

TAMPS	Tactical Aircraft Mission Planning System
TDSP	tamper detection support program
T/E	Table of Equipment (as in material allowances)
TECHEVAL	Technical evaluation
TED	Trunk Encryption Device
TEK	Traffic Encryption Key
TFS	traffic flow security
TISCOM	Telecommunication and Information Systems Command
TN	transaction number
TPA	Terminal Privilege Authority
TPC	Two-Person Control
TPI	Two-Person Integrity
TRANSEC	transmission security
TRI-TAC	Tri-service Tactical Communications System
TRI	Transfer Report Initiating
TRR	Transfer Receipt Report
TRRA	Transfer Receipt Report All
TRRE	Transfer Receipt Report Exception
TRRI	Transfer Receipt Report Individual
TSCM	technical surveillance countermeasures
TSCO	Top Secret Control Officer
TSE	technical security evaluation
TSEC	telecommunications security

TYCOM	Type Commander
UAS	User Application Software
UNODIR	unless otherwise directed
UR	User Representative
USNDA	United States National Distribution Authority
UV	Unique Variable (key)
VDLS	Vault, Depot, and Logistic Systems
VGA	video graphics array
WAN	Wide Area Network
WETS	warehouse equipment tracking system
WHENDI	when directed
XEU	Xerox Encryption Unit

ANNEX C

CONTROLLING AUTHORITIES FOR COMSEC MATERIAL

1. Purpose:

This Annex describes the appointment and responsibilities of DON organizations performing Controlling Authority (CONAUTH) functions for COMSEC keying material. It also describes those functions and lists options for reacting to emergency or crisis situations and provides guidance for evaluating reported COMSEC incidents.

CONAUTHs **must** ensure messages related to; implementation of new short titles, changes to status information or to the application or proper usage of keying material, emergency supersession's and hazardous conditions (HAZCONs) are sent to NCMS Washington DC//N3//, CMIO Norfolk VA, DIR TIER1 San Antonio, TX, CSLA TIER1 and DIRNSA FT George G Meade MD//I31107//, and all accounts validated for the material.

2. Controlling Authority Appointment, Training and Designation Requirements:

a. Whenever a new cryptonet/circuit is established, a CONAUTH will be identified to manage the operational use of keying material assigned to the cryptonet/circuit. Normally, the command requesting establishment of a new cryptonet/circuit will be designated the CONAUTH for the designated keymat.

b. The CONAUTH is normally organizationally senior to all cryptonet members. When the CONAUTH is not, all members must still abide by any direction given to the cryptonet by the CONAUTH.

c. For electronic key generated locally, the Commander that directed the key generation performs the CONAUTH functions, unless those functions are specifically delegated in writing to another organization. (As stated in Article 740, accounts will not generate ALC-6 material without prior authorization from NCMS)

d. Personal fulfilling the responsibilities of a Controlling Authority must;

1. Meet the same minimum grade requirements as an EKMS Manager set forth in Article 412 herein.

2. Possess a security clearance equal to or higher than the highest classification of material the person has/requires access to.

3. Be designated in writing by the CO, OIC, or SCMSRO, as applicable. A separate appointment letter is not required for EKMS Managers performing CONAUTH duties. A single statement on the appointment letter can satisfy this requirement, i.e. "As the Controlling Authority for keying material managed by XXXXXXXX (organization title), including locally generated ALC-7 material, you will familiarize yourself and perform the duties outlined in Annex C of reference (a). Appointment letters will be retained locally at the appointing organization.

4. Complete the NSA Controlling Authority computer-based training (CBT) within 60 days of assumption of CONAUTH responsibilities. The CBT is available on the SIPRNET at: www.ia.nsa.smil.mil/iaservices/cawg/training/index.cfm.

5. In the Key Management Infrastructure (KMI), CONAUTHs who are not KOAMs must possess a minimum final SECRET clearance, complete the NSA Controlling Authority CBT discussed above, meet the grade requirements discussed in 2.d.1 above and meet and comply with the KMI registration and enrollment policies and Operational Security Doctrine (OSD) for the management client (MGC). Product Requestors who meet the same requirements as a CONAUTH in KMI may validate orders or allowance changes, when authority for doing so has been delegated, in writing by the CONAUTH.

6. Changes to CONAUTHs must be communicated to all organizations reflected in Paragraph 1 including accounts validated for the material. This will be done via official message and updating CAD data will not be used for this purpose. CAD data reflects Account Managers however; some CONAUTHS are not EKMS Managers.

3. **Controlling Authority Responsibilities:**

a. Designates the cryptonet members and coordinates with the appropriate distribution organizations including CMIO, CSLA TIER1, DIR TIER1, NCMS, and DIRNSA regarding establishment and support of the cryptonet (i.e., identifying the EKMS/COMSEC accounts to be distributed the keying material, the implementation date of the key, the number of copies distributed and reporting changes to cryptonet configuration).

b. Promulgates effective and supersession information, including the directing of emergency supersession, when warranted, authorizes transfers or destruction and cancels short titles under their cognizance when no longer required, as applicable. CONAUTHs will promulgate status messages on a monthly, quarterly, semi-annual, annual basis or as required based on the frequency of supersession of the material reflected.

For ALC-7 material generated locally and transferred, the generating account will originate an effective date transaction and send the transaction to the account the ALC-7 material was transferred to via the X.400 message server. Procedures for the origination and distribution of effective date transactions can be found in EKMS-704. Do not send effective date transactions for locally generated ALC-7 material to the COR.

c. Approves classification changes to keying material managed and notifies each organization reflected in Paragraph (1) above via official message of the change.

d. Specifies the key change time when it is not stated in the keying material format. The selected time must be consistent throughout the cryptonet and chosen to have the least operational impact. If changed, the CONAUTH is responsible for notifying all accounts validated for the material prior to the change. **Failure to do so may adversely impact the mission of the holders or result in a cryptographic incident.**

e. Recommends changes in system design (e.g., the content or format of the keying material) and submits recommendations to DIRNSA//I31107// via the COR and the operational chain of command. Net members or key holders must be notified in writing of changes to the application or usage of the key. Example: Use of keying material previously produced in physical form with a particular diagraph in a manner that is no longer consistent with the diagraph, i.e. diagraph GF (quarterly) now used as a GC (monthly) or VF (quarterly) now used a VA (daily). Except in emergencies, CONAUTHS will not change supersession rates without proper coordination.

f. Makes spare group assignment in operations codes, as required.

g. Authorizes in non-emergent situations reproduction of COMSEC material (key or books) for the purpose of transferring to another account or issuing the material to LE personnel of another account. See Article 781 of this manual for guidance and applicable reporting when reproduction is done to fulfill an urgent operational requirement.

h. Reports faulty keying material (i.e., production errors) to DIRNSA, DIR TIER1, CSLA TIER1, info NCMS//N5// and CMIO.

i. Directs holders to keep faulty keying material pending disposition instructions from DIRNSA.

j. Ensures faulty keying material is returned to DIRNSA (account 880099) via DCS for forensic examination, when directed.

k. Conducts an annual review of short titles under the cognizance of the CONAUTH. This includes; (1) responding to requests from NCMS for an annual review of all short titles managed to confirm a continuing operational requirement exists for the keying material. Results of the annual review will be reported to the organizations reflected in Paragraph (1) herein less validated accounts and will include up-to-date POC information to include; name, message PLA, phone numbers, unclassified and classified email addresses, and the URL to the CONAUTHS web site where status information is posted, if applicable. The annual review should focus on:

(1) Identification of short titles which may be placed in contingency status. (Ex: Large cryptosystems with a history of low usage during peacetime).

(2) Cancellation of short titles and providing disposition instructions to accounts validated for the material when the cryptonet/circuit supported has been cancelled. All short title cancellation messages must also include disposition instructions for copies of the short title(s) held or in transit to validated accounts and will be addressed to the organizations reflected in Paragraph (1) above.

(3) Verification that reserve keying material is adequate for unexpected cryptonet requirements.

(4) Verification that the format and application of the key is correct and consistent with any associated diagraph or status messages.

l. Assesses the security impact of reports of physical incidents of material under the CONAUTHs purview and provide a compromise assessment. See Chapter 9 for reporting COMSEC incidents and guidance for assessing compromise probability.

m. When a compromise is declared, notify the all organizations reflected in Paragraph 1. Ensure DIRNSA FT GEORGE G MEADE MD//I31132// is an info addee on such messages if compromise occurs as a result of tampering.

n. Directs emergency supersession of keying material when required. Emergency supersession **must** be coordinated with DIRNSA, NCMS, CMIO, DIR TIER1, and CSLA TIER1.

o. NCMS and NSA must consider the following factors when directing emergency supersession:

(1) The format of the material, i.e. physical vs. electronic and the number of editions held in reserve at the user level.

(2) The ability of DIRNSA to produce additional keying material and the ability of distribution authorities to supply replacement editions in a timely manner.

(3) The time required for notification of all cryptonet members and implementation of the replacement material.

p. Authorizes reuse of prematurely used segments when the requesting EKMS account lacks an adequate amount of the current edition of COMSEC material to re-key the equipment.

4. **Evaluating Reports of COMSEC Physical Incidents Involving COMSEC Keying Material**:

a. Guidelines for Evaluating COMSEC Physical Incidents. COMSEC incident evaluation is often a subjective process, even when the CONAUTH is in possession of all pertinent facts. See Article 980 for compromise probability assessments.

b. Time Limits for Evaluating COMSEC Incidents. CONAUTHs are responsible for the collection and review of any information required in rendering an evaluation. COMSEC incident reports must be evaluated within the time limits specified below based on the precedence of the initial report. Time limits begin with receipt of the initial report, or amplifying report if the initial report does not contain sufficient information to permit an evaluation.

Message Precedence	**Response Time**
IMMEDIATE	24 Hours
PRIORITY	48 Hours
ROUTINE	5 Working Days

c. Cryptoperiod Extensions.

Traditional keying material has both an effective period and a crypto period. The effective period pertains to the edition of the material whereas the crypto period pertains to the duration an individual segment, page, table, etc… is authorized for use. **Example**: An edition may; (a) supersede monthly and the segments which make up the edition have a daily cryptoperiod or (b) supersede quarterly and the segments which make up the edition have a weekly cryptoperiod. The examples in the previous sentence correlate to material produced in the AA and ZB diagraphs.

When operationally required to do so and such is not prohibited by the Operational Security Doctrine (OSD) for the device, the CONAUTH may extend crypto periods as follows:

(1) Off-line systems (e.g., call signs, operational codes, authenticators) up to 72 hours.

(2) Auto-manual/machine crypto systems (e.g., KL 51, KG 81, KG 84, and KY 57/58) up to (7) days.

With the approval of the CO, NCSs and net subscribers may extend the cryptoperiod up to two hours to complete a transmission in progress at key change time. These extensions do not require CONAUTH approval or notification. In a tactical environment CONAUTHs may extend cryptoperiods up to 30 days.

(3) Extensions other than those described above, must be granted by NSA 410-854-6831, (DSN) 244-6831 or after hours at 301-688-3495 (DSN) 644-3495 to the CONAUTH. When verbally granted by NSA, the CONAUTH must record; the date/time of the authorization, the short title, edition and segment (as applicable), when the extension expires, and the NSA POC, including contact data who granted the extension.

d. Action Required When COMSEC Keying Material has Been Compromised or Suspected Compromised. When a possible compromise has occurred and the CONAUTH is determining if an emergency supersession is warranted or such may not be feasible, the CONAUTH may declare a Hazardous Condition (HAZCON) in writing and notify all holders to minimize communications which are secured using the key. If declared, the CONAUTH must specify when the HAZCON will end.

Alternatively, when substantial evidence exists indicating keying material has been compromised, the Controlling Authority may elect not to issue a HAZCON but instead direct an emergency supersession. A sample message can be found in Figure C-1.

e. Resupply Considerations and Possible Methods.

Prior to directing an emergency supersession, the CONAUTH **must** coordinate with NCMS//N3//, CMIO, and DIRNSA //I31107// to ensure that profiles or allowances are adjusted and re-supply actions are initiated for physical material. CONAUTHs are responsible for notification to all accounts validated for the material affected by the emergency supersession. A sample message can be found in Figure C-2.

AMD-9

NOTE: Account Managers (EKMS Managers/KOAMs) are ~~responsible for providing~~ required to provide up-to-date status information to support LEs including but not limited to; HAZCONS, emergency supersession's or changes to key usage.

Superseding electronically generated key presents a unique problem for mobile/tactical users in that some of the communications paths used to deliver the key may no longer exist, because some of the relaying units may have redeployed and can no longer serve in that capacity.   Consequently, before directing supersession, CONAUTHs must take into consideration the time needed to create or reestablish communications paths.

(1) **When supersession is warranted but not all net members hold or can be supplied with replacement key**, the following options are available to the CONAUTH:

(a) Distribute keys in Black (encrypted) form via SIPR as an attachment.

(b) OTAD (SKL or DTD/STE) or OTAT.

(c) Direct the early implementation of uncompromised future editions by those cryptonet members who hold those editions or can be supplied quickly, and exclude from net operations those members who do not hold or cannot be furnished the replacement material.

(c) Physically transfer key to net members in an electronic storage device (DTD/SKL/TKL). When protecting key and the CIK is inserted or accessible, the device must be afforded protection at the same classification as the key or data protected, the higher of the two.

(d) Key transferred to units other or issued to LE personnel from another organization or service requires the consent of the Controlling Authority, except as indicated in Article 675 to this manual.

f. Action Required When Supersession is not Feasible.

When supersession is warranted but not feasible, the following options are available to the CONAUTH:

(1) Extend the cryptoperiod of uncompromised keying material using the guidelines specified in Tab-1 of this Annex as follows:

(2) Suspend operations of the cryptonet until key can be resupplied.

(3) Continue to use compromised key. This action is a **last** resort when normal supersession of the compromised material will take place before emergency supersession can be accomplished, or where keying material changes would have a serious detrimental effect on operations, or where replacement material is not available.

(a) The CONAUTH must alert net members by any secure means available, including issuing a HAZCON that a possible compromise has occurred and direct net members minimize transmissions using the compromised key.

(b) This option should be resorted to only when continued operation of the cryptonet is critical to mission accomplishment. CONAUTHs will direct traffic reviews of record traffic encrypted in compromised keying material when warranted.

5. **Designating Contingency Keying Material**:

a. When large amounts of crypto materials are provided for regular consumption and are destroyed unused, the CONAUTH should consider placing the material in a WHENDI status and designating the key as contingency key.

b. Contingency keying material is material held for use under specific operational conditions or in support of specific contingency plans.

c. The material is not implemented until needed for the specific requirement, and is not destroyed until after use.

6. **COMSEC Keying Material Support to Allied Nations.**

a. Controlling Authorities who are required to provide allied nations with COMSEC keying material for use in U.S. COMSEC equipment must ensure compliance with this manual and the guidance set forth in CNSSI 1002.

b. The providing of COMSEC keying material among participants in a multinational coalition is permitted when all the following conditions are met:

1. The receiving nation has been granted formal authorization from the appropriate content owners to access the information on the circuit.

2. The CONAUTH of the keying material has approved the specific nations and units to be part of the cryptonet and documented this in the Key Management Support Plan (KMSP), OPTASK LINK, OPTASK COMM, COMSEC Call-Out Message or equivalent.

3. The equipment supported by the keying material has been approved for release to the allied nation by NSA/DP22 and the Committee on National Security Systems (CNSS).

c. Upon verification of compliance with paragraph 5.a above, strict adherence to proper transfer or issuing procedures, and consent of the Controlling Authority[1], keying material may:

1. Be distributed directly from any U.S. COMSEC account to any foreign COMSEC account.

2. Be distributed from any foreign account directly to a U.S. COMSEC. **NOTE:** U.S. use of foreign keying material in U.S. equipment requires approval from NSA/DP2 and NCMS.

[1] During actual wartime operations or imminent conflict, Military Commanders may direct the issue of Theater-specific keying material to units not previously validated for the material. Theater-specific U.S. keying material may also be provided to allied/coalition forces which have obtained the equipment requiring the keying material through DP22 and approved CNSS procedures. When allied/coalition forces are provided U.S. keying material other units on the circuit must be made aware of the non-U.S. presence on the net to prevent disclosure of information which is not

releasable. In either scenario, if prior authorization was not possible, the CONAUTH must be notified within 72 hours.

When feasible, keying material should be sent electronically to international partners through either the International EKMS (IEKMS) or the NATO Military Committee Distribution and Accounting Agency (DACAN) or equivalent.

3. The use of approved OTAT or OTAD procedures and appropriate keying material and transmission media is also authorized for electronic delivery of keying material when the provider and recipient are capable and trained on proper procedures, including security and logging requirements.

4. Key may also be provided through direct loading of an electronic fill device provided by the allied partner. Proper local custody procedures must be adhered to.

c. Requests to use U.S.-produced keying material in foreign-produced equipment should be referred through NCMS to NSA //DP2/IE31//.

7. **COMSEC Keying Material Support to Contractor (87XXXX) Accounts**.

a. Controlling Authorities are not authorized to release or authorize the release of keying material to contractor accounts without first obtaining Service Authority approval required by Article 505.g to this manual and OPNAVINST 2221.5(series).

b. NCMS will provide Service Authority approval via official record message or digitally signed email.

c. Upon approval of the Service Authority, the CONAUTH may approve or disapprove the request. Service Authority approval does not replace the requirement for CONAUTH for approval or disapproval of the release material to a contractor account. The Service Authority is responsible for ensuring the request is consistent with the regulations mentioned in Paragraph 7.a above.

d. If approved by the Service Authority and the CONAUTH, the CONAUTH is responsible for notifying DIRNSA to have the 87XXXX account added to the distribution profile for the material.

SAMPLE HAZARDOUS CONDITION (HAZCON) MESSAGE

(**NOTE**: CLASSIFIED WHEN FILLED IN)

FROM: CONTROLLING AUTHORITY
TO: ALL VALIDATED ACCOUNTS (CRYPTONET MEMBERS)
INFO: DIRNSA FT GEORGE G MEADE MD//I311071/I3113//
NCMS WASHINGTON DC
CSLA TIER1
CLSA TIER1 SAN ANTONIO TX
CMIO NORFOLK VA (NAVY/USMC/USCG/MSC ACCOUNTS)
COMSEC CHAIN OF COMMAND (OF ALL CRYPTONET MEMBERS)
BT
CLASSIFICATION (MINIMUM CLASSIFICATION OF CONFIDENTIAL)
MSGID/GENADMIN/CONTROLLING AUTHORITY OFFICE SYMBOL)/-/MONTH//
SUBJ/HAZARDOUS CONDITION (HAZCON)
REF/A/GENADMIN/(VIOLATING UNIT)/(INITIAL REPORT DTG)/
REF/B/DOC/NCMS WASH DC/05APR2010//
NARR/REF A IS INITIAL REPORT OF A COMSEC INCIDENT INVOLVING AKAD-0000, EDITION PAPA JULIET (PJ), SEGMENTS 2-54; 57-58, 61-62; 65-68 AND USKAD-0000, EDITION INDIA X-RAY (IX), SEGMENTS 2-31. REF B IS EKMS-1(SERIES)//
POC/(NAME)/(POSITION/TITLE)/(LOCATION)/(TELEPHONE)/(SIPR EMAIL)//
RMKS/1. (C) BASED ON INFORMATION CONTAINED IN REF A, AKAT/D-0000 EDITION PJ, AND USKAT/D-0000 EDITION IX ALONG WITH LISTED SEGMENTS ARE LOST AND SUBJECT TO COMPROMISE. IAW ANNEX C TO REF B, AKAT/D-0000 EDITION PJ AND USKAT/D-0000 EDITION IX ARE HEREBY PLACED IN A HAZCON STATUS UNTIL (APPLICABLE DATE). FLT CREWS AND USERS MAY CONTINUE TO USE AKAT/D-0000 AND USKAT/D-0000, BUT SHOULD BE AWARE THAT THE ABOVE MENTIONED SEGMENTS HAVE BEEN LOST AND SUBJECT TO COMPROMISE.

2. (U) THIS HAZCON EXPIRES (APPLICABLE DATE).
DOWNGRADING/DECLASSIFY INSTRUCTIONS.

BT

FIGURE C-1

SAMPLE EMERGENCY SUPERSESSION MESSAGE

(**NOTE**: CLASSIFIED WHEN FILLED IN)

FROM: CONTROLLING AUTHORITY
TO: AUTHORIZED USERS (CRYPTONET MEMBERS)//
INFO: DIRNSA FT GEORGE G MEADE MD//I311071/I3113//
NCMS WASHINGTON DC
CSLA TIER1
CLSA TIER1 SAN ANTONIO TX
CMIO NORFOLK VA (NAVY/USMC/USCG/MSC ACCOUNTS)
COMSEC CHAIN OF COMMAND (OF ALL CRYPTONET MEMBERS)
BT
CLASSIFICATION (MINIMUM CLASSIFICATION OF CONFIDENTIAL)
MSGID/GENADMIN/CONTROLLING AUTHORITY OFFICE SYMBOL)/-/MONTH//
SUBJ/COMSEC INCIDENT CASE NUMBER (OFFICE SYMBOL) NR. XXX-XX//
REF/A/GENADMIN/(VIOLATING UNIT)/(INITIAL REPORT DTG)//
REF/B/GENADMIN/DIRNSA/I3113/(DTG)//
REF/C/DOC/NCMS WASH DC/(DTG)
NARR/REF A IS INITIAL REPORT OF A COMSEC INCIDENT. REF B IS DIRNSA EVALUATION MESSAGE. REF C IS EKMS-1(SERIES)//
POC/(NAME)/(POSITION/TITLE)/(LOCATION)/(TELEPHONE)/(SIPR EMAIL)//
RMKS/1. (C) REF A REPORTED LOSS OF AN/CYZ-10(V3) DATA TRANSFER DEVICE (DTD) AND ASSOCIATED CIK. THE DTD WAS LOADED WITH AKAT/D-0000 AND USKAT/D-0000. REF B ASSESSED THIS INCIDENT AS "COMPROMISE."

(ABOVE LINE EXPLAINS WHY SUPERSESSION IS NEEDED)

2. (C) EFFECTIVE 0001Z (07 MAR 07), USKAT/D-0000, EDITION INDIA XRAY (IX) WILL BE SUPERSEDED AND AUTHORIZED FOR DESTRUCTION.

(ABOVE LINE EXPLAINS WHAT WILL BE SUPERSEDED)

3. (U) THE NEW EFFECTIVE PERIODS FOR USKAT/D-0000 ARE REFLECTED BELOW:

A. (U) EDITION	EFFECTIVE DATE	DESTROY
(1) (C) INDIA YANKEE	(07-31 MAR 07)	(01 APR 07)
(2) (C) INDIA ZULU	(01-30 APR 07)	(01 MAY 07)

4. (C) USKAT/D-0000 IS A DAILY KEY AND USERS WILL BEGIN EDITION INDIA YANKEE (IY) ON SEGMENT 7. SEGMENTS 1 THRU 6 OF EDITION INDIA YANKEE (IY) ARE SUBSEQUENTLY AUTHORIZED FOR DESTRUCTION.

(ABOVE LINE FOR SPECIAL AND DISPOSITION INSTRUCTIONS)
5. (C) AKAT/D-0000, EDITION PAPA JULIET (PJ) WILL NOT, REPEAT, NOT BE SUPERSEDED DUE TO THE BRIDGE FROM THE LAST DAY OF THE CURRENT MONTH TO THE FIRST DAY OF THE NEXT MONTH.

(ABOVE LINE FOR OTHER SPECIAL INSTRUCTIONS)

6. (U) FOLLOW ON EDITION STATUS WILL BE REFLECTED IN THE NEXT STATUS MESSAGE PROMULGATED BY ORIGINATOR.//

DECLASSIFY/DOWNGRADING INSTRUCTIONS

BT

FIGURE C-2
TAB 1 TO ANNEX C TO EKMS 1B

GUIDELINES FOR EXTENDING CRYPTOPERIODS

When cryptoperiods must be extended for reasons other than logistics needs (e.g., under pre-strike, battlefield, or field training conditions), CONAUTHs are encouraged to conduct a risk assessment prior to implementing the extension and should consider the following before making a decision as to the length of time the cryptoperiod will be extended.

Size of the Cryptonet. The key used on a large cryptonet is usually more vulnerable to compromise than the key used on a small cryptonet because it is available at more locations and more people have access to it. Also, large nets generally carry higher volumes of traffic than small nets. The compromise of a key used to secure a large net could make more intelligence available to an adversary. For this reason, CONAUTHs must keep their cryptonets as small as operationally feasible.

Location and Operating Environment of Net Members. Net members located in the United States, its territories, and its protectorates are normally at less risk than those in other locations. Net members located in high risk environments, (areas outside the United States where there is a small or no United States or allied military presence or where the political climate is unstable, have an increased risk of physical compromise. Mobile and tactical users have a greater opportunity for loss, particularly undetected loss of material than do fixed plant net members. In addition, loss on the battlefield could pose an immediate threat not only to United States communications but also to United States lives.

Sensitivity and Perishability of Traffic. The CONAUTH should consider the classification of the protected information and whether the information is of long or short term intelligence value. Compromise of a key used to secure upper level strategic communications would have a more devastating effect on United States security than would compromise of a key used to secure highly perishable or lower level tactical communications.

TAB 1 TO ANNEX C TO EKMS 1B (CONT'D.)

Emergency Supersession Plan. The CONAUTH must have a plan to affect timely replacement of compromised key and know approximately how quickly the key can be replaced if the plan is realistic and addresses also a worst case scenario. The plan should be tested because it is extremely difficult to accomplish an unscheduled rekey in a large net without creating additional problems and confusion. The CONAUTH must know the logistic channels that support the cryptonet as well as the electronic key transfer or distribution capabilities of the associated equipment.

Operation Impact of an Extended Cryptoperiod. The CONAUTH must make an assessment as to whether extending the cryptoperiod is for operational necessity or for operator convenience. If we do not follow standard procedures during wartime, the value of our peacetime training is questionable. Feedback from personnel involved in combat operations indicated operators were, at times confused by changes in operational procedures.

If cryptoperiod extensions are necessary to maintain critical communications during battle (actual or field training), the following guidelines apply:

- Begin all pre-planned cryptoperiods with a new key setting.
- Extend cryptoperiods by net and not by short title, whenever possible.
- Re-key all affected nets as soon as there is a break in activity.

ANNEX D

HELPFUL URLs

The URLs contained herein are intended to assist KOAM personnel in obtaining: status information; information related to KMI including Computer Based Training (CBT) material; KMI related forms; modernization information related to CCI equipment and related algorithms; and other information which, if consulted may enhance the management of the account. NCMS has no administrative privileges or operational responsibility for the availability or content hosted on the sites reflected herein other than the NCMS portal(s).

Status Information

NCMS has published a listing of many Controlling Authorities and the URLs to where their status information is posted on the SIPRNET. The file titled "**Helpful URLs for COMSEC Account Managers**" also contains hyperlinks to various OPTASKs, OPORDS and Communication Information Advisories and Bulletins (CIAs/CIBs). The file can be found on the NCMS (SIPR) Share Point Portal listed below. Hyperlinks for SIPR URLs below have been removed to properly display the correct path.

General & Other Information

Controlling Authority Computer-Based Training (CBT):
www.ia.nsa.smil.mil/iaservices/cawg/training/index.cfm

Defense Courier Service (DCS) Customer Service Manual and USTC Form-10: http://www.transcom.mil/

Information Assurance Workforce (IAWF) Certification Resource page: https://www.portal.navy.mil/cyberfor/iawf/default.aspx.

KMI CPA, CPSO AND TSO Computer-Based Training (CBTs) and other information:
http://www.ia.nsa.smil.mil/iaservices/programs/km/kmi_program_office/programdocs/suitabilitydocs.cfm

MGC Operators Manual:
http://www.ia.nsa.smil.mil/iaservices/programs/km/kmi_program_office/programdocs/suitabilitydocs.cfm

AMD-9

~~NCMS (SIPR) Share Point portal:
www.fleetforces.navy.smil.mil/netwarcom/ncms/ekmsmanagers/default.aspx~~

NSA Classified Material Conversion (CMC):
http://www.nsa.gov/cmc/

NSA KMI (SIPR) Portal:
http://www.iad.nsa.smil.mil/iaservices/km/kmi_program_office/programdocs/suitabilityDocs.cfm

NSA Master Reference Catalog (A good tool for Short Title and Controlling Authority look ups)
http://secure.ia.nsa.smil.mil/iaservices/cawg/mrc/index.cfm

NSA Media Destruction Guidance (including the Evaluated Products List (EPL))
http://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml

Operational Security Doctrine (OSD) for CCI equipment:
www.iad.nsa.smil.mil – IA Library – Doctrine

Protected Security Services (PSS). A list of commercial carriers which provides PSS can be obtained via email to:
SDDC.OPS.CarrReg@us.army.mil

ANNEX E

STATUS OF COMSEC MATERIAL REPORT (SCMR)

```
                        STATUS OF COMSEC MATERIAL REPORT (SCMR)
                                09-JUN-2009 19:00:03

                                          Effect     Disp        Disp
S/T  Designator Edition        Amend    Date       Date        Code   ALC
       ------------ -------        -------  --------    -------     ------ ----
AKAT  23235  Description:  KG-84 A/C Operational OTAR KEK Keytape   Class:   T    Area:   WP
          Cntrl  Auth:  NCTAMS  EASTPAC  HONOLULU  HI             Effect Period:   1YR
          Remarks:

          H                       20090601   20100601    DAL    1

AKAT  34346     Description:  KG-84 Operational Keytape                Class:   S    Area:   WW
          Cntrl Auth:   DCA  WASHINGTON  DC                      Effect Period: 1YR
          Remarks:

           A                       WHENDI                 DAL    1
           B                       WHENDI                 DAL    1

AKAT  45457     Description:  KG-84  A/C  Operational  OTAR KEK  Keytape Class:   S    Area:  EP
          Cntrl  Auth:  NCTAMS  EASTPAC  HONOLUL HI                Effect Period: 1M
          Remarks:

           E                       20090901   20091001    DAL    1
           F                       20091001   20091101    DAL    1

     Class:   T  =  Top Secret     S  =  Secret     C  =  Confidential     U  =  Unclassified

        ALC:     1  =  AL1         2  =  AL2           4  =  AL4          6 = AL6
      Area:     A  =  Atlantic     P  =  Pacific       WW  =  Worldwide   WP = Westpac
                EP =  Eastpac      M  =  Mediterranean IO  =  Indian  Ocean
```

ANNEX E

STATUS OF COMSEC MATERIAL REPORT (SCMR)

1. **General**:

a. The Status of COMSEC Material Report (SCMR) is classified SECRET NOFORN and, is produced by the COR and provided to Tier 2 accounts automatically each month via their X.400 mailboxes.

b. This report should be used in conjunction with any messages from Controlling Authorities throughout the month for the most current status information and prior to conducting COMSEC material destruction. However, destruction will be based on the most current status information promulgated by the Controlling Authority. When conflicting information is found (i.e. errors, incorrect information, material held but not listed, material listed but not held), contact NCMS N3 Key Division. (See Annex S for point of contact information) or the Controlling Authority.

2. **Content**: Each short title of COMSEC material listed on the SCMR will provide the following information:

a. Edition
b. Effective date (e.g., 20090901)
c. Supersession date, (e.g., 20090101)
d. Disposition date (e.g., DAL)
e. Accounting legend code (ALC)
f. WHENDI flag
g. Edition classification
h. Cryptoperiod destruction delay
i. Cancellation date
j. Controlling Authority
k. Handling restrictions
l. Associated equipment/devices
m. Remarks
n. Supersession rate
o. Disposition code
p. MATCODE
q. Account name

3. **Short title explanations**: The following explains the short titles on the example page of a SCMR presented earlier:

a. The first short title example, AKAT 23235 edition "H” is classified TOP SECRET, used in WESTPAC, and has an effective period of one (1) year. This short title is effective 20090601 and authorized for destruction 20100601

b. In the second short title example, none of the editions of AKAT 34346 are authorized for use. The "WHENDI" (when directed) means that until the CONAUTH (DCA WASH DC) notifies all holders of the date that each edition is effective for use, the material must not be used.

c. In the third short title example, AKAT 45457 edition "E" is effective 20090901 and authorized for destruction on 20091001. Edition "F" is effective 20091001 and authorized for destruction on 20091101.

4. **Effective period**: Terms used to indicate the effective period are as follows:

a. D: Preceded by a number that indicates the number of days the edition is effective (e.g., 3D, 10D, 15D).

b. M: Preceded by a number that indicates the number of months the edition is effective (e.g., 1M, 2M, 3M).

c. Y: Preceded by a number that indicates the number of years the edition is effective (e.g., 1YR).

NOTE: Disregard any other letters other than D, M, and Y. If the "Effective period" field is blank, the effective period is indefinite or not known.

5. **CAUTION**: NEVER destroy COMSEC equipment without specific written guidance from NCMS//N3//, except in the case of emergency destruction.

ANNEX F

LCMS ACCOUNTABLE ITEMS (A/I) SUMMARY

UNCLASSIFIED

LCMS provides a utility to review a list of accountable items in the local account or issued to a local element registered in LCMS. The operator can print an inventory summary, view the detailed attributes associated with an accountable item, or review the item's material history. Additionally, the data displayed can be filtered by the type of material, i.e. All, Traditional, Modern, Equipment and Aids.

The Element Selection window shows the EKMS ID and name of the local account, all registered sub-accounts and Local Elements for which the local account is responsible.

The Current Accountable Items window shows a list of all the short title/editions of accountable material for the selected element. Separate entries are provided for the same Short Title/Edition/ALC with different classifications [applicable to Modern key]. Only the summary quantity of the Short Title/Edition/ALC/Classification is shown.

> **NOTE: The inventory summary is not considered to be an an Inventory Report. The AIS will reflect all ALC 1,2,4,6 and 7 COMSEC material (including modern key such as NES) held by the account. An up-to-date printout of the AIS will be maintained by the manager in the chronological file IAW ANNEX T.**

ANNEX G

EKMS ACCOUNT ESTABLISHMENT REQUEST

1. **Purpose**: A request to establish an EKMS account is to be submitted only when it is not possible to draw needed materials from an existing EKMS account (either within the organization or located in close proximity thereto). The request will be submitted after appointment of a qualified EKMS Manager and Alternate(s) and fulfillment of the requirements in paragraph 2 below.

2. **ISIC requirements**: A command's ISIC must perform the following prior to a subordinate command submitting a request to establish an EKMS account:

a. Validate requirement for the EKMS account.

b. Validate command compliance with the minimum physical security requirements for safeguarding COMSEC material. See Chapter 5 for **physical security requirements.**

c. Determine the required COMSEC material based on command mission and communications capabilities.

d. Obtain CONAUTH authorization for COMSEC material not listed in a standard allowance instruction (e.g., for USN afloat units - CLF/CPF/CINCUSNAVEURINST C2282.1 (series)).

3. **Lead time**: A minimum of 45 days is required to establish an EKMS account and to provide the initial COMSEC material.

4. **Submission**: A letter or message must be forwarded to the appropriate addressees listed in Article 405.e.(3). All correspondence for NCMS must contain the office code //N31//.

5. **Preparation guidance**: The following information must be provided in the account establishment request:

a. Command title, mailing address, ISIC, HCI, ISIC authorization to establish the account and validation that the command meets physical security requirements for storing COMSEC material.

b. CONAUTH validation. (**N/A when material is listed in a standard allowance instruction (e.g., CLF/CPF/CINCUSNAVEURINST C2282.1 (series)).**

c. Period material is required (permanent or temporary). Specify exact dates only when required on a temporary basis.

d. Specify date material required (DMR) at the command.

e. Shipping instructions. (**Identify DCS station, COR, or provide alternative shipping instructions (e.g., material will be picked up from CMIO Norfolk or USNDA**).

6. **Delivery of material**: After submitting a request to establish an EKMS account, the requesting command must:

a. Coordinate with the area DCS station and establish a DCS account if picking up material.

b. Submit a CMS Form 1 to CMIO Norfolk **ONLY** if the command will be picking up material from the CMIO. (**Annex H contains instructions for submitting a CMS Form 1**).

ANNEX G

EKMS ACCOUNT ESTABLISHMENT REQUEST (SAMPLE MESSAGE)

```
R 101830Z AUG 09 ZYB
FM PRECOMUNIT RANGER
TO COMPACFLT PEARL HARBOR HI//N633//
INFO NCMS WASHINGTON DC//N3//
CNO WASHINGTON DC//N2/N6F1133//
COMNAVAIRPAC SAN DIEGO CA//N321//
CSLA TIER1 DIR TIER1 SAN ANTONIO TX//
CMIO NORFOLK VA//N3//
DIRNSA FT GEORGE G MEADE MD//I31//
SPAWARSYSCEN ATLANTIC CHARLESTON SC//80P/526CS/721SR//
BT
UNCLAS//N02280//
MSGID/GENADMIN/PCU RANGER/-/AUG//
SUBJ/EKMS ACCOUNT ESTABLISHMENT//
REF/A/DOC/NCMS/-//
REF/B/LTR/COMNAVAIRPAC N321/1MAY09//
REF/C/DOC/CLF/CPF/CINCUSNAVEURINST C2282.1/-//
REF/D/GENADMIN/DIRNSA/050403ZAUG09//
NARR/REF A EKMS-1(SERIES).  REF B PROVIDES CERTIFICATION AUTHORIZATION
TO STORE CLASSIFIED/COMSEC MATERIAL AND AUTHORIZES EKMS ACCOUNT
ESTABLISHMENT. REF C IS CLF/CPF/CNE STANDARD SHIPBOARD ALLOWANCE
PUBLICATION. REF D IS CONTROLLING AUTHORITY VALIDATION.//
POC/SAILOR/CTOC/DSN: 123-4567/EMAIL:SAILOR(AT)CVN70.NAVY.MIL//
RMKS/1.   REQUEST ESTABLISHMENT OF AN EKMS ACCOUNT TO SUPPORT
OPERATIONAL REQUIREMENTS. FOLLOWING INFORMATION PROVIDED IAW ARTICLE
REF A ARTICLE 405 AND ANNEX G:
   A.   COMMAND TITLE:             PCU RANGER  (CV-61)
   B.   COMMAND UIC:               12345
   C.   MAILING  ADDRESS:          USS RANGER  (CV-61)
                                   COMM  DEPT
                                   FPO AP 96631
   D.   COMMAND PLA:               PCU RANGER//OFFICE CODE//
   E.   ISIC AND VALIDATION REF:   COMNAVAIRPAC; REF B GERMANE.
   F.   HCI: TOP SECRET.
   G.   COMMAND MEETS STORAGE/PHYSICAL SECURITY REQUIREMENTS FOR
        STORING TOP SECRET MATERIAL AS VALIDATED BY REF B.
   H.   EKMS MANAGER:               CTOC SAILOR
        PHONE NUMBER COMM/DSN
        EMAIL ADDRESS
   I.   ALT MANAGER:                IT1 SHIPMATE
        PHONE NUMBER COMM/DSN
        EMAIL ADDRESS:
2.   REQUIRED MATERIAL:
   A.   KEYING MATERIAL:
      (1)    AFLOAT UNITS SUBMIT REQUESTS FOR MATERIAL IAW REF C.
      (2)    ASHORE UNITS CONTACT ISIC AND CONAUTH
   B.   MANUALS/EQUIP/RELATED DEVICES:
```

(1) AFLOAT UNITS SUBMIT REQUESTS FOR MATERIAL IAW REF C.
(2) ASHORE UNITS CONTACT ISIC AND/OR CONAUTH, AS APPLICABLE.
C. VALIDATION AUTHORITY/JUSTIFICATION: REF D GERMANE.
3. DMR: 100424
A. DURATION: TEMPORARY 100424-101024
B. SHIPPING INSTRUCTIONS: MTL WILL BE PICKED UP AT CMIO NORFOLK.//

NOTE: USCG/USMC/MSC ACCOUNTS MUST ENSURE THEIR SERVICE COMPONENTS ARE INCLUDED IN ALL ACCOUNT ESTABLISHMENT OR DISESTABLISHMENT MESSAGES. SEE ANNEX S **FOR POC DATA AND PLAs.**

ANNEX H

CMS FORM 1

____
(DDMMYY)

From: ____
____
(Command title and mailing address)

To: CMIO Norfolk

Subj: **AUTHORIZATION TO RECEIPT FOR AND COURIER COMSEC MATERIAL**

Ref: (a) EKMS 1 (series)

1. Per reference (a), the below named individuals are authorized to drop-off, receipt for and courier COMSEC material for the above EKMS numbered account command:

RATE/RANK/ GRADE	NAME (Last, First, MI)	DOD ID	SECURITY CLEARANCE	POSITION	SIGNATURE

---LAST ENTRY---

2. a. **EKMS ID number:** __________
   b. **Highest Classification Indicator (HCI):** ______
   c. Command Telephone number(s): COMM: (   )____________
   DSN: ________________
   d. **ISIC:** ____________________________

3. I certify that the individuals identified above are assigned to my command; are authorized to drop-off, receipt for and courier COMSEC material for the above command/account; and possess a security clearance equal to or higher than that of the COMSEC material being handled.

AUTHORIZING OFFICIAL SIGNATURE: ________________________________

RANK/GRADE NAME (Last, first, MI) POSITION (e.g., CO, OIC)

____

____

(CMS Form 1)

NOTE: By direction signatures are not authorized.

1. **Purpose**: CMS Form 1 is a locally prepared form that is used to authorize appropriately cleared personnel, one of whom must be the EKMS Manager or Alternate, to receipt for and courier COMSEC material between their command and CMIO. It must be submitted on command letterhead, official naval message or digitally signed **and** encrypted email.

NOTE: CMS Form 1 is required ONLY if material will be picked up from CMIO.

2. **Preparation**: All information, less signatures, must be typed or printed (in black/blue-black ink); signatures must be signed on both copies of CMS Form 1 in black/blue-black ink.

a. **Date**: Enter the date the authorizing official signs the form.

b. **Command title and address**: Enter the command name and complete mailing address.

c. **Authorized personnel**: Enter the required information and have each individual verify the information by affixing their signature. Enter "LAST ENTRY," immediately below the last name.

d. **EKMS ID number, HCI, telephone numbers, and ISIC**: Enter the required information.

e. **Authorizing official signature and data**: The authorizing official must be the CO, OIC, or SCMSRO of the EKMS account command or the designated individual acting on their behalf.

3. **Submission**: The CMS Form 1 must be submitted via letter or via digitally signed and PKI encrypted email. In the event of a short-fused emergent operational requirement, a message containing the same information as a CMS Form 1 may be submitted in order to receipt for and courier COMSEC material. Use of a message does not negate the requirement for an account to ensure that CMIO holds a valid CMS Form 1. **Do not fax CMS Form-1s or send them as attachments to unencrypted email.**

4. **Disposition**: Forward the original copy of CMS Form 1 to CMIO and retain the second copy in the CMS

Chronological File.

5. Changes: Whenever there is a change in the authorizing official or the personnel authorized to receipt for and courier COMSEC material, a new CMS Form 1 must be submitted.

6. CMIO Action: Retain CMS Form 1 on file for each EKMS/COMSEC account. Ensure that COMSEC material is received from/released only to personnel that are listed on a valid CMS Form 1.

ANNEX I

USTRANSCOM FORM 10

Defense Courier Account Record

Part 1: All Account Types

Account Delivery Address	Account Mailing Address and Fax Number	After Duty Hours Contact	Account Expiration Date
		Organization/Group NIPR and SIPR E-Mail NIPR: SIPR:	

Customers must coordinate with their servicing Defense Courier Station if there are any additions and/or deletions concerning the authorizing official or the individuals named below.

Name	Grade/Rank	Telephone Number E-Mail Address	Signature

Clearance statement: The authorizing official acknowledges that the individuals listed above are authorized to enter and receive qualified material IAW DODI 5200.33; and possess an appropriate personal security clearance for the qualified material they will be entering or receiving.

Date	Authorizing Official (Name, Grade, Title) E Mail:	Rotation Date	Signature

Part 2 for Government Contractor Accounts: THIS CERTIFIES THAT THE INDIVIDUALS IDENTIFIED HEREIN POSSESS A VALID SECURITY CLEARANCE TO THE DEGREE OF THE HIGHEST CLASSIFIED MATERIAL THAT COULD BE RECEIVED AND/OR ENTERED BY THE ACCOUNT.

Date	Government Security verification authority (Name/Grade/Position/Organization) E Mail:	Signature

Part 3 for Consolidated Control Account (CCA) Authorization:
PERSONNEL LISTED ON THE USTRANSCOM FORM 10 FOR LISTED ARE AUTHORIZED TO ENTER/RECEIVE MATRIAL ON BEHALF OF THE ACCOUNT (S) LISTED IN PART 1.

Courier Account Number -
Station run Code (DODAAC)

Date	Authorizing Official (Name, Grade, Title) Email:	Rotation Date	Signature

Part 4 Forces Afloat Required Contact Information

Point of Contact	**POTS Number (Surface Vessels)**	**Commercial/DSN**	**E-Mail Address**
Operations Officer			
Executive Officer			
Account Validation (For Courier Station Use Only) **Validating Courier (Name and Grade)**	**Date**	**Signature**	

ANNEX J

SAMPLE APPOINTMENT LETTER/MEMORANDUM

____
(DDMMYY)

From: Commanding Officer
To: (Rank/Rate/Grade), Name, and DOD ID

Subj: **APPOINTMENT LETTER/MEMORANDUM**

Ref: (a) EKMS 1 (series)

1. In accordance with reference (a), you are hereby appointed as (EKMS Manager, Alternate EKMS Manager, Local Element (Issuing), STE User Representative, LMD UNIX System Administrator, or EKMS Clerk) for this command.

2. **EKMS account number:** __________.

3. EKMS COI (V-4C-0013) completed on (YYMMDD) at (name/location of EKMS COI), as applicable. If a quota has been obtained but training not yet completed, annotate the class convening date and prepare an updated Appointment Letter or affix the completion certificate to the Appointment Letter when training is completed.

4. **Security clearance:** (Top Secret/Secret, etc., as applicable).

5. Following designation requirements contained in (Article 412) of reference (a) are waived:

a. ____
b. ____
(identify authority for and specific requirement(s) waived; if no requirements waived, indicate "N/A")

____
(Signature of Commanding Officer)

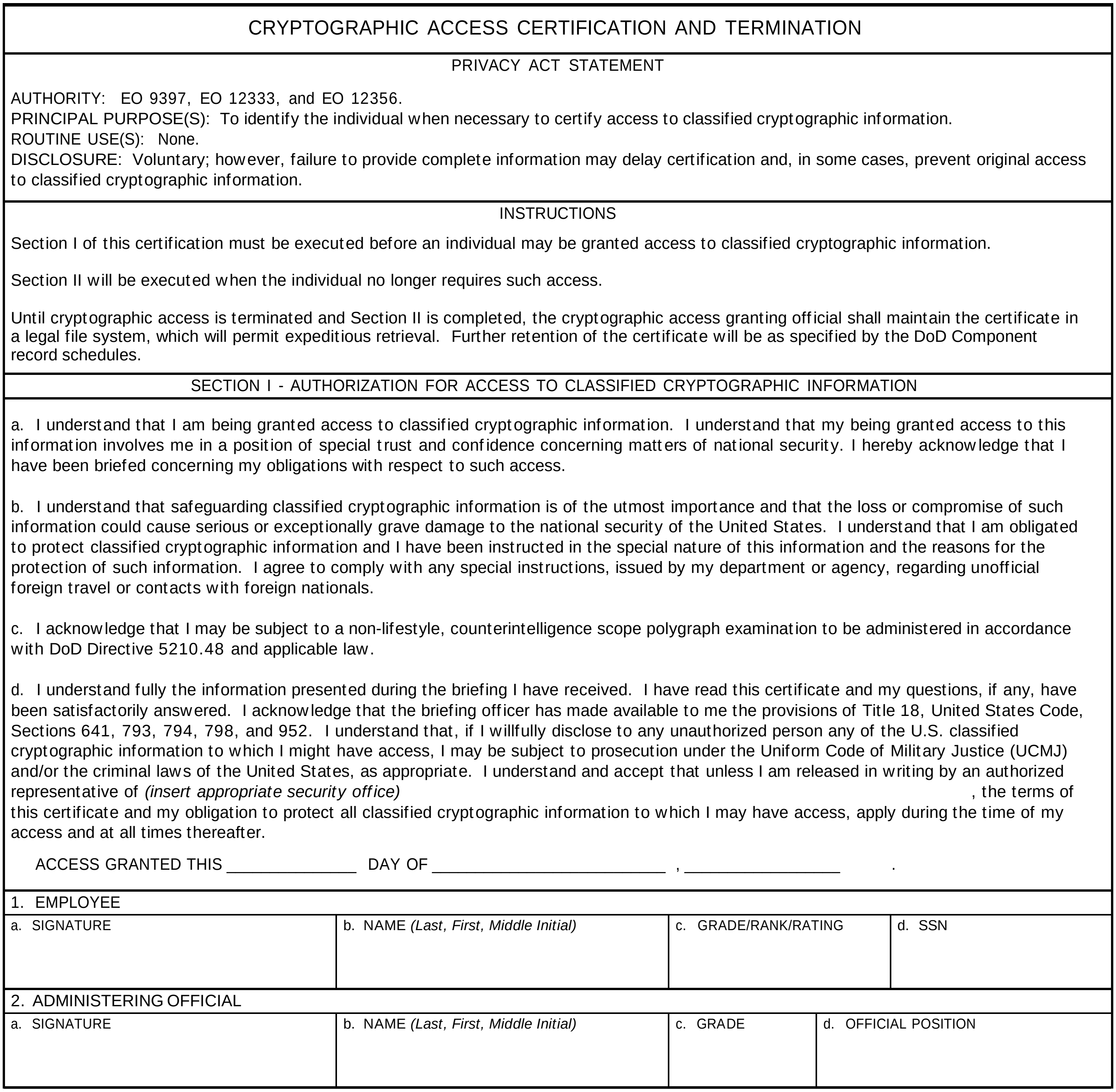
NOTES: 1. Retain the original copy of the letter/memorandum of appointment Correspondence/Message File for two years from the date an individual has been relieved of his/her

duties.

2. Do <u>not</u> forward individual letter/memorandum of appointment to the COR or NCMS.

ANNEX K

SD FORM 572



CRYPTOGRAPHIC ACCESS CERTIFICATION AND TERMINATION

PRIVACY ACT STATEMENT

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.

INSTRUCTIONS

Section I of this certification must be executed before an individual may be granted access to classified cryptographic information.

Section II will be executed when the individual no longer requires such access.

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.

SECTION I - AUTHORIZATION FOR ACCESS TO CLASSIFIED CRYPTOGRAPHIC INFORMATION

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.

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.

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.

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 *(insert appropriate security office)* , 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.

ACCESS GRANTED THIS ______________ DAY OF _________________________ , ________________ .

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

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).

ACCESS WITHDRAWN THIS ____________ DAY OF ____________________ __________________, .

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

SD FORM 572, JUN 2000 PREVIOUS EDITION IS OBSOLETE.

SAMPLE
CRYPTOGRAPHIC ACCESS BRIEFING

You have been selected to perform duties that will require access to U.S. classified cryptographic information. It is essential that you be made aware of certain facts relevant to the protection of this information before access is granted. You must know the reason why special safeguards are required to protect U.S. classified cryptographic information. You must understand this directive, which requires these safeguards and the penalties you may incur for the unauthorized disclosure, unauthorized retention, or negligent handling of U.S. classified cryptographic information under the criminal laws of the United States. Failure to properly safeguard this information could cause serious or exceptionally grave damage, or irreparable injury, to the national security of the United States; or could be used to advantage by a foreign nation.

U.S. classified cryptographic information is especially sensitive because it is used to protect other classified information. Any particular piece of cryptographic keying material and any specific cryptographic technique may be used to protect a large quantity of classified information during transmission. If the integrity of a cryptographic system is breached at any point, all information protected by the system may be compromised. The safeguards placed on U.S. classified cryptographic information are a necessary component of government programs to ensure that our nation’s vital secrets are not compromised.

Because access to U.S. classified cryptographic information is granted on a strict need-to-know basis, you will be given access to only that cryptographic information necessary in the performance of your duties.

Especially important to the protection of U.S. classified cryptographic information is the timely reporting of any known or suspected compromise of this information. If a cryptographic system is compromised, but the compromise is not reported, the continued use of the system can result in the loss of all information protected by it. If the compromise is reported, steps can be taken to lessen an adversary’s advantage gained through the compromise of the information.

You should know that intelligence services of some foreign governments prize the acquisition of U.S. classified cryptographic information. They will go to extreme lengths to compromise U.S. citizens and force them to divulge cryptographic techniques and materials that protect the nation's secrets around the world. You must understand that any personal or financial relationship with a foreign government's representative could make you vulnerable to attempts at coercion to divulge U.S. classified cryptographic information. You should be alert to recognize those attempts so that you may successfully counter them. The best personal policy is to avoid discussions that reveal your knowledge of, or access to, U.S. classified cryptographic information and thus avoid highlighting yourself to those who would seek the information you possess. Any attempt, either through friendship or coercion, to solicit your knowledge regarding U.S. classified cryptographic information must be reported immediately to (insert appropriate security office).

In view of the risks noted above, unofficial travel to designated countries may require the prior approval of (insert appropriate security office). It is essential that you contact (insert appropriate security office) if such unofficial travel becomes necessary.

Finally, you must know that, should you willfully or negligently disclose to any unauthorized persons any of the U.S. classified cryptographic information to which you will have access, you may be subject to administrative and civil sanctions, including adverse personnel actions, as well as criminal sanctions under the Uniform Code of Military Justice (UCMJ) and/or the criminal laws of the United States, as appropriate.

ANNEX L

SAMPLE LETTER/MEMORANDUM OF AGREEMENT (LOA/MOA)

When the CO of a Local Element (LE) is different from the CO of the parent account (numbered account providing COMSEC material support), a Letter or Memorandum of Agreement (LOA/MOA) is required between the two commands. The **sample** letter below outlines the minimum content required to be addressed; however, additional provisions may be included at the discretion of the CO of the supporting account.

From: Commanding Officer (EKMS numbered account command)
To: Commanding Officer (Local Element command)

Subj: COMSEC MATERIAL LETTER OF AGREEMENT

Ref: (a) (cite letter request for material support)
(b) EKMS 1 (series)

Encl: (1) (cite the locally prepared command COMSEC instruction)

1. In response to reference (a), this command agrees to provide COMSEC material support to your command with the following provisions:

a. **Compliance with Enclosure (1)**: The Local Element will ensure that all personnel authorized to handle and use the COMSEC materials provided by this command comply with the guidance contained in reference (b) and enclosure (1). To this end, the Local Element will conduct training sessions at regular intervals on the proper handling, accounting, use and safeguarding of COMSEC materials. Particular emphasis must be given to educating personnel in how to identify COMSEC incidents and Practices Dangerous to Security (PDS).

b. **Reporting of COMSEC Incidents**: In the event of a COMSEC incident, the Local Element will report the incident to the addressees outlined in reference (b) and will include this command as an information addressee on the initial report and any amplifying reports.

OR

Reporting of COMSEC Incidents: In the event of a COMSEC incident, the Local Element will report the incident immediately to this command and the Local Element CO. The information provided must be of sufficient detail to enable this command to assume responsibility for reporting the incident.

c. **Responsibility for Certifying Clearances/Access**: The Local Element will accept full responsibility for ensuring that all personnel whose duties require them to use COMSEC materials are properly cleared and that the privileges assigned formally authorize access to COMSEC material. The Local Element will also require personnel who are issued/have access to COMSEC material complete a ~~COMSEC Responsibility Acknowledgment~~ SD Form 572 as required by reference (b). AMD-9

d. **Issuing COMSEC material in Electronic Form**: For electronic COMSEC material issues, the Local Element will provide a Data Transfer Device (DTD, Simple Key Loader (SKL) or Tactical Key Loader (TKL) with sufficient storage capability. LE personnel must be knowledgeable in the usage and capabilities of the DTD, SKL, or TKL, as applicable.

e. **Notification of Local Element Appointments**: This command will be notified of new Local Element appointments and changes in Local Element positions held. This notification will consist of forwarding the original copy of the Appointment Letter/Memorandum as contained in Annex J of EKMS 1 (series). This command will also be notified, in writing, when a Local Element has been relieved of his/her duties.

f. **Storage/Facility Clearance**: The Local Element command will provide this command with written certification that the storage facility (i.e., safe and/or vault) of the Local Element is approved for storage of the highest classification of COMSEC material to be stored.

g. **Spot Checks**: The Local Element will ensure compliance with training and spot check requirements set forth in reference (b). Copies of completed training and spot checks will be provided the EKMS Manager of the supporting account.

h. **Inventory Requirements**: The Local Element will comply with inventory requirements as outlined in reference (b) Articles 766.a.3.d, 766.a.4 (note), 775 and 778, as applicable.

i. **Emergency Action Plan/Emergency Destruction Procedures**: The Local Element command will ensure that procedures are established and tested for Emergency Action and Emergency Destruction, as applicable in accordance with reference (b), enclosure (1) and the Local Elements command, installation commander or higher instruction.

ANNEX M

EMERGENCY PROTECTION OF COMSEC MATERIAL

1. **Purpose**: This Annex prescribes policy and procedures for planning, protecting, and destroying COMSEC material during emergency conditions. It is the responsibility of the EKMS Manager to maintain the COMSEC material portion of the Command Emergency Action Plan.

2. **Emergency Protection Planning**:

a. Every command that holds classified COMSEC or CCI material must prepare and maintain a current, written emergency plan for safeguarding such material in the event of an emergency.

b. For commands located within the U.S. and its territories planning must consider natural disasters (e.g., fire, flood, tornado, and earthquake) and hostile actions (terrorist attack, rioting, or civil uprising).

c. For commands located outside the U.S. and its territories and deployable commands, planning must include both an Emergency Action Plan (EAP) for natural disasters and an Emergency Destruction Procedures (EDP) for hostile action.

d. All activities located within the U.S and its territories that hold classified COMSEC or CCI material will maintain an up-to-date, written Emergency Action Plan for the protection of COMSEC material appropriate for natural disasters likely to occur in their region of the country (e.g., hurricanes in the South, tornados and floods in the mid-West, wild fires in the West, etc.). In addition, all activities located within the U.S and its territories will have conducted an initial written risk assessment and must maintain an up-to-date copy of the risk determination document that assesses the potential for hostile actions against their facilities (such as terrorist attack, rioting, or civil uprising). Based on the sensitivity of the operations, or the facility, the cognizant security official will either certify that the review has determined no need for the Emergency Plan to consider hostile actions, or, if it is determined that a potential risk exists, develop EDPs for inclusion in their Emergency Plan.

e. The head of any department or agency may, at their discretion, direct any facility to create an Emergency Plan that considers hostile action, regardless of local risk. Government Contracting Officers may also direct that the Emergency Plan for contractor facilities consider hostile action.

f. Planning for hostile actions must concentrate on procedures to safely evacuate or securely destroy the COMSEC material, to include providing for the proper type and a sufficient number of destruction devices to carry out emergency destruction. Planning for hostile action shall also include the necessary training for all individuals who might perform emergency destruction. By contrast, planning for natural disasters should be directed toward maintaining security control over the material until the situation stabilizes, taking into account the possible loss of normal physical security protection that might occur during and after a natural disaster. The operating routines for COMSEC facilities should be structured so as to minimize the number and complexity of actions that must be taken during emergencies to protect COMSEC material. **For example**:

(1) Only the minimum amount of COMSEC material should be held at any one time; i.e., routine destruction should be conducted frequently and excess COMSEC material disposed of in accordance with department or agency directives. COMSEC requirements should be reviewed at least annually to validate need for material on hand.

(2) COMSEC material should be stored and inventoried in ways that will facilitate emergency evacuation or destruction.

g. Emergency protection of classified COMSEC and CCI material applies to U.S. Government contractor facilities, other U.S. non-governmental entities who produce or hold COMSEC material, and any other facilities that are designed to provide a backup COMSEC capability (whether U.S. Government or contractor owned).

h. Planning for acts of terrorism is much more difficult but must concentrate on maintaining security control over the material, evacuation of the material, and/or secure destruction.

i. These plans will be incorporated into the overall Emergency Action Plan (EAP)/Emergency Destruction Plan (EDP) of the command.

j. All Emergency Plans will be reviewed annually and updated as necessary, or whenever changes in the local environment dictate an update to the plan.

k. Efficient planning and training, which involving every individual who uses COMSEC material, increases the probability of preventing its loss or compromise during an emergency.

l. The command EAP/EDP, if not specific to LE operations, must be modified or annexed to include specific actions to be taken by LEs.

m. Any detachment that operates independently (i.e., aircraft and communications/special purpose vans) from their parent command should have their own unique EAP/EDP specifically tailored for those times of independent operation. In all cases, they should be included in the command's EAP/EDP.

3. **Guidelines For Minimizing Actions**:

a. Hold only the minimum amount of COMSEC material at any time (i.e., routine destruction should be conducted frequently and excess COMSEC material disposed of as directed by appropriate authorities).

b. Store COMSEC material to facilitate emergency removal or destruction (e.g., separate COMSEC material from other classified material, and segregate COMSEC keying material by status, type and classification).

NOTE: COMSEC material which has been designated for "NATO" use is not exclusively NATO material but is, in fact, COMSEC material. Consequently, this material need not be separated from other COMSEC material but must be stored and segregated by status and classification.

c. As emergency situations develop, initiate precautionary destruction or evacuation of all material not immediately needed for continued operational effectiveness. After destroying material, notify appropriate authorities so they may begin re-supply planning.

4. **Preparedness Planning For Disasters**: Planning for disasters must provide for:

a. Fire reporting and initial fire fighting by assigned personnel.

b. Assignment of on-the-scene responsibility for ensuring protection of the COMSEC material held.

c. Security or removing classified COMSEC material and evacuating the area(s).

d. Protection of material when admission of outside emergency personnel into the secure area(s) is necessary.

e. Assessment and reporting of probable exposure of classified COMSEC material to unauthorized persons during the emergency.

f. Post-emergency inventory of classified COMSEC and CCI material and reporting any losses or unauthorized exposure to appropriate authorities.

5. **Preparedness Planning for Hostile Actions**: Planning for hostile actions must take into account the possible types of situations that may occur (e.g., an ordered withdrawal over a specified period of time, a hostile environment situation where destruction must be carried out in a discrete manner to avoid triggering hostile actions, or fully hostile imminent overrun situations.). Ensure that the plan provides for the following:

a. Assessing the threat of occurrence of the various types of hostile emergencies at the particular activity and of the threat that these potential emergencies pose to the COMSEC material held.

b. The availability and adequacy of physical security protection capabilities (e.g., perimeter controls, guard forces, and physical defenses) at the individual buildings and other locations when COMSEC material is held.

c. Facilities for effecting emergency evacuation of COMSEC material under emergency conditions, including an assessment of the probable risks associated with evacuation.

NOTE: Except under extraordinary conditions (e.g., an urgent need to restore secure communications after relocation), COMSEC keying material should be destroyed rather than evacuated.

d. Facilities and procedures for effecting secure emergency destruction of COMSEC material must address:

(1) Adequate number of destruction devices

(2) Availability of electrical power

(3) Secure storage facilities nearby

(4) Adequately protected destruction areas

(5) Personnel assignments

(6) Clear delineation of responsibilities for implementing emergency destruction

e. Precautionary destruction of COMSEC material, particularly maintenance manuals (KAMs) and keying material not operationally required to ensure continuity of operations during the emergency.

(1) In a deteriorating situation all "full" maintenance manuals (i.e., contains cryptographic logic information) which are not absolutely essential for continued mission accomplishment must be destroyed.

(2) When there is insufficient time under emergency conditions to completely destroy such manuals, every reasonable effort must be made to remove and destroy their sensitive pages (i.e., those containing cryptographic logic/classified schematics).

NOTES: 1. Sensitive pages in U.S. produced KAMs are listed on fold-out Lists of Effective Pages at the rear of other textual portions.

2. Some KAMs further identify their sensitive pages by means of gray or black diagonal or rectangular markings at the upper portion of the binding edge.

(a) To prepare for possible emergency destruction of sensitive pages from KAMs in areas or situations where capture by hostile forces is possible, comply with the following guidance:

1 Apply distinctive markings (e.g., red stripes) to the binder edge and covers of all KAMs containing identified sensitive pages.

2 Remove the screw posts or binders rings,

or open the multi-ring binder, whichever is applicable.

3 Remove each sensitive page from the KAM and cut off the upper left-hand corner of the page so that the first binder hole is removed. Care must be taken not to delete any text or diagram.

(b) Should it become necessary to implement emergency destruction, the sensitive KAM pages may be removed as follows:

1 Remove the screw posts or binders rings, or open the multi-ring binder and remove all pages from the KAM.

2 Insert a thin metal rod (e.g., wire or screwdriver) through the remaining top left-hand hole of the document.

3 Grasp the rod in both hands and shake the document vigorously; the sensitive pages should fall out freely.

f. Establishment of emergency communications procedures.

(1) External communications during emergency situations should be limited to contact with a single remote point.

(2) This point will act as a distribution center for outgoing message traffic and a filter for incoming queries and guidance.

(3) When there is warning of hostile intent and physical security protection is inadequate to prevent overrun of the facility, secure communications should be discontinued in time to allow for thorough destruction of all classified COMSEC and CCI material, including classified and CCI elements of COMSEC equipment.

6. **Preparing The Emergency Plan**:

a. The person who is most aware of the extent and significance of the COMSEC material on hand should prepare the emergency plan.

b. The Commanding Officer or other responsible official must be aware of and approve the emergency plan.

c. If the plan calls for destroying COMSEC material, all destruction material, devices, and facilities must be readily available and in good working order.

d. The plan must be realistic, workable, and accomplish the goals for which it is prepared. Factors that will contribute to this are:

(1) All duties under the plan must be clearly and concisely described.

(2) All authorized personnel at the command should be aware of the existence of the plan.

(a) Each individual assigned duties under the plan must receive detailed instructions on how to carry out those duties when the plan is implemented.

(b) All personnel should be familiar with all duties so that changes in assignment may be made, if necessary. This may be accomplished by periodically rotating the emergency duties of all personnel.

(3) Training exercises will be conducted annually (quarterly exercises are recommended) to ensure that everyone, especially newly assigned personnel who might have to take part in an actual emergency, will be able to carry out their duties.

NOTE: If necessary, the plan should be modified based on based on the training exercise results.

(4) The three options available in an emergency are: <u>securing</u> the material, <u>removing</u> it from the scene of the emergency, or <u>destroying</u> it. Planners must consider which of these options may be applicable to their command.

(5) For example, if it appears that a civil uprising is to be short lived, and the COMSEC facility is to be only temporarily abandoned, the actions to take could be:

(a) Ensure that all superseded keying material has been destroyed.

(b) Gather up the current and future keying material and take it along.

(c) Remove classified and CCI elements from crypto-equipment and lock them, along with other classified COMSEC material, in approved storage containers.

(d) Secure the facility door(s), and leave.

(e) Upon return, conduct a complete inventory.

NOTE: If it appears that the facility is likely to be overrun, the emergency destruction plan should be put into effect.

7. **Emergency Destruction Planning**: Three categories of COMSEC material that may require destruction in hostile emergencies are: COMSEC keying material, COMSEC-related material (e.g., maintenance manuals, operating instructions, and general doctrinal publications), and equipment.

a. **Precautionary Destruction List A**: When precautionary destruction is necessary, destroy keying material and non-essential manuals in accordance with this Annex and the EAP/EDP.

b. **Complete Destruction Priority Lists B & C**: When sufficient personnel and facilities are available, assign different persons to destroy the material in each category by means of separate destruction facilities and follow the priorities listed herein as incorporated into your EAP/EDP.

NOTE: When personnel and/or destruction facilities are limited, join the three categories and destroy the material following the priorities listed in Priority List C.

8. **Emergency Destruction Priorities**:

a. **Precautionary Destruction Priority List A**:

(1) Superseded keying material and secondary variables.

(a) TOP SECRET primary keying material.

(b) SECRET, CONFIDENTIAL, and UNCLASSIFIED primary keying material.

(2) Future (reserve on board) keying material for use one or two months in the future.

(3) Non-essential classified manuals:

(a) Maintenance manuals.
(b) Operating manuals.
(c) Administrative manuals.

b. **Complete Destruction Priority List B**: When sufficient personnel and facilities are available, destroy COMSEC material in the following order:

(1) Keying Material:

(a) All superseded keying material designated CRYPTO, except tactical operations and authentication codes classified below SECRET.

(b) Currently effective keying material designated CRYPTO including key stored electrically in crypto equipment and FDs (see paragraph c. below regarding STE or KSV-21 material), except unused two-holder keying material and unused one-time pads.

(c) Zeroize all STE keying material held by the account in the following order:

1. Operational Keying Material designated TOP SECRET, SECRET, CONFIDENTIAL, UNCLASSIFIED.

2. Seed Keying Material – TOP SECRET, SECRET, CONFIDENTIAL, UNCLASSIFIED.

(d) TOP SECRET multi-holder (i.e., more than two holders) keying material marked CRYPTO which will become effective within the next 30 days.

(e) Superseded tactical operations codes classified below SECRET.

(f) SECRET and CONFIDENTIAL multi-holder keying material marked CRYPTO which will become effective within the next 30 days.

(g) All remaining classified keying material, authentication systems, maintenance, and unused one-time pads.

(2) **COMSEC Aids**:

(a) Complete COMSEC equipment maintenance manuals or their sensitive pages. When there is insufficient time to completely destroy these manuals, every reasonable effort must be made to destroy their sensitive pages.

(b) National, department, agency, and service general doctrinal guidance publications.

(c) Status documents showing the effective dates for COMSEC keying material.

(d) Keying material holder lists and directories.

(e) Remaining classified pages of maintenance manuals.

(f) Classified cryptographic and non-cryptographic operational general publications (e.g., AMSGs, NAGs and SDIPs).

(g) Cryptographic Operating Instructions (KAOs).

(h) Remaining classified COMSEC documents.

(3) **Equipment**: Make a reasonable effort to evacuate equipment, but the immediate goal is to render them unusable and un-repairable.

NOTE: Although it is desirable to destroy jeopardized crypto-equipment so thoroughly that logic reconstruction is impossible, this cannot be guaranteed in most field environments.

(a) Zeroize the equipment if the keying element cannot be physically withdrawn.

(b) Remove and destroy readily removable classified elements (e.g., printed-circuit boards).

(c) Destroy remaining classified elements.

NOTE: Unclassified chassis and unclassified elements need not be destroyed.

(d) Zeroize all loaded STEs held by the account in the following order based on the level of keying material loaded into the terminal: TOP SECRET, SECRET, CONFIDENTIAL, UNCLASSIFIED.

NOTE: If lack of power prohibits keying material(FDs)(KSD-64As)) or a loaded terminal from being zeroized, ensure that all keying material and CIKs are physically removed from the area. In extreme emergencies, an attempt to physically destroy fill devices and CIKs is allowed. Material can be burned or broken as much as possible to prevent unauthorized use. It should be noted that the effectiveness of these methods has not be documented.

c. **Complete Destruction Priority List C**: In cases where personnel and/or facilities are limited, follow the destruction priority list below:

(1) All superseded and currently effective keying material marked CRYPTO (including key stored electrically in crypto-equipment and fill devices), except tactical operations codes and authentication systems classified below SECRET, unused two-holder keying material, and unused one-time pads.

(2) Superseded tactical operations codes classified below SECRET.

(3) Complete COMSEC equipment maintenance manuals or their sensitive pages.

(4) Classified general COMSEC doctrinal guidance publications.

(5) Classified elements of COMSEC equipment.

(6) Remaining COMSEC equipment maintenance manuals and classified operating instructions.

(7) Remaining classified COMSEC material.

(8) Future editions of multi-holder (i.e., more than two holders) keying material and current but unused copies of two-holder keying material.

9. **Conducting Emergency Destruction**: Any of the methods approved for routine destruction of classified COMSEC material may be used for emergency destruction.

a. **Printed Matter**:

(1) Destroy keying material and other classified COMSEC publications beyond reconstruction.

(2) Destroy all "full" maintenance manuals (i.e., those containing cryptographic logic information/classified schematics). When time does not permit, every reasonable effort must be made to remove and destroy their sensitive pages in accordance with paragraph 5.e.

b. **Classified Crypto-Equipment**: Render classified crypto-equipment inoperable (i.e., beyond reuse).

(1) If time permits, destroy the cryptographic logic of the equipment beyond reconstruction by removing and destroying the classified portions of the equipment, which include certain printed circuit boards and multi-layer boards and keyed permuting devices.

(2) If these classified elements are destroyed, it is not necessary to destroy the remainder of the equipment.

c. **Emergency Destruction in Aircraft**: When time or facility limitations preclude complete destruction of COMSEC material aboard aircraft, make all reasonable efforts to prevent the material from falling into unauthorized hands.

(1) When the aircraft is operating over water and an emergency or forced landing is imminent, zeroize the COMSEC equipment, shred or tear up the keying material, and disperse it. If feasible, remove the classified elements from the equipment and smash and disperse them.

(2) If an aircraft is in danger of making an emergency landing in friendly territory, zeroize the equipment and keep all the COMSEC materials in the aircraft.

(3) If the aircraft is being forced or shot down over hostile territory, zeroize the equipment, then shred or tear up and disperse the keying material, and make all reasonable efforts to remove, smash, and disperse the classified equipment components.

d. **Emergency Destruction Aboard Ship**:

(1) If the ship is in imminent danger of sinking in a U.S.-controlled area, zeroize the equipment, destroy all COMSEC material as completely as possible in the time available, lock it in security containers and permit it to sink with the ship.

(2) If the ship is in imminent danger of capture or

of sinking in an area where foreign elements would have salvage opportunities, destroy all COMSEC equipment and all keying material.

(a) Destroy all COMSEC equipment as completely as time permits, and jettison the undestroyed or partially destroyed COMSEC material overboard.

(b) Place paper items and other material that could float in weighted canvas bags before jettisoning.

e. **Emergency Destruction in Mobile Communication Vehicles:**

(1) When time or facility limitations preclude complete destruction of COMSEC material located in the vehicle, make all reasonable efforts to prevent the material from falling into unauthorized hands.

10. **Reporting Emergency Destruction**:

a. Accurate information relative to the extent of an emergency is absolutely essential to the effective evaluation of the COMSEC impact of the occurrence, and is second in importance only to the completeness of the destruction.

b. The Commanding Officer/OIC or official responsible for safeguarding COMSEC material, which has been subjected to emergency destruction, is responsible for reporting the attendant facts to the appropriate seniors in the chain of command by the most expeditious means available.

(1) **Reporting Instructions**: The senior official shall report the facts surrounding the destruction to CNO//N614//, NCMS//N5//, DIRNSA//I31132//, and both operational and administrative command echelons as soon as possible; if feasible, use a secure means of reporting.

(2) **Required Information**: State in the report the material destroyed, the method and extent of destruction, and any classified COMSEC material items presumed compromised (e.g., items either not destroyed or not completely destroyed).

NOTE: Follow the reporting procedures for COMSEC Incidents as outlined in Chapter 9. Ensure the EAP/EDP includes guidance for providing the required information.

ANNEX N

CONSTRUCTION SPECIFICATIONS FOR STORAGE VAULTS

1. **Purpose**:

a. To provide minimum standards for the construction of vaults used as storage facilities for COMSEC keying material.

b. The specifications included in this Annex are not prescriptive because there are other construction techniques which will provide equivalent protection, which may be required to meet certain operational requirements.

c. Modular Vault Systems are an alternative to traditional vault construction when time and portability are primary concerns and are discussed in TAB-1 of this Annex.

2. **Vault Construction Specifications**:

a. **Floors and Walls**: Eight inches of reinforced concrete to meet current structural standards. Walls must extend to the underside of the roof slab.

b. **Roof**: The roof should be a monolithic reinforced concrete slab of a thickness to be determined by structural requirements, but not less than the walls and floors.

c. **Ceiling**: The roof or ceiling shall be reinforced concrete of a thickness to be determined by structural requirements, but not less than the floors and walls.

NOTE: Where the existing roof does not conform to the vault roof requirements stated above, a vault roof structurally equal to the vault walls shall be constructed.

d. **Door and Frame Unit:** The vault door and frame shall conform to Federal Specification AA-D-2757, Class 8 vault door, or Federal Specification AA-D-600, Class 5 vault door. Doors shall be equipped with a built-in GSA-approved combination lock meeting Federal Specification FF-L-2740.

e. **Lock**: The combination lock shall conform to the Underwriters' Laboratories, Inc., Standard No. 768. The specific lock model used shall bear a valid UL Group 3R11 label.

NOTE: All vault doors procured after 14 April 1993 must be equipped with a GSA approved combination lock that meets the requirements of Federal Specifications FF-L-2740.

3. **Day Gate**: If desired, the vault door unit of a storage vault may include a day gate of the standard make by a manufacturer, and the doorframe may be designed to accommodate the day gate.

a. The gate shall be of the swing-in hinged type with not less than 1/2 inch diameter vertical rods.

b. The gate frame shall be of not less than 3/8 by 1 1/2 inch steel members. It shall be equipped with a locking device arranged to permit locking and unlocking of the gate from the inside.

4. **Structural Design**: In addition to the requirements given for walls, floors, and roof construction, construction shall be in accordance with nationally recognized standards of structural practice.

5. **Safety and Emergency Devices**: Although the provision of an emergency escape device on a vault door tends to weaken the security provided by the vault, such a device may be required in order to adequately provide for personnel safety.

a. **Minimum safety requirements**: All vaults shall be equipped with:

(1) A luminous-type light switch

(2) An emergency light if the vault is otherwise unlighted.

(3) An interior alarm switch or device (e.g., telephone, radio, or intercom) to permit a person in the vault to communicate with the vault custodian, guard, or guard post so as to obtain his/her release.

(4) A decal containing emergency instructions on how to obtain release must be permanently affixed to the inside of the door or elsewhere prominently displayed inside the vault.

b. **Emergency escape device**:

(1) If an emergency escape device is considered necessary, it shall be permanently attached to the inside of the door and

shall not be activated by the exterior locking device or otherwise accessible from the outside.

(2) The device shall be designed and installed so that drilling and rapping the door from the outside will not give access to the vault by activating the escape device.

(3) The device shall meet the requirements of paragraph 3.3.9 of GSA Federal Specification AA-D-00600 (GSA-FSS), concerning an exterior attack on the door.

c. Ventilation: If an emergency escape device is not provided, the following approved Underwriters Laboratories (UL), Inc., devices must be installed in each vault:

(1) A UL Bank Vault Emergency Ventilator

(2) At least one UL approved fire extinguisher situated in a position near the vault door

NOTE: These provisions are recommended, even if an emergency escape device is provided.

TAB-1 TO ANNEX N TO EKMS 1B

MODULAR VAULT SYSTEMS

1. **Modular Vault Systems (MVSs)**: MVSs are fabricated using pre-manufactured interlocking panels and connecting hardware. The GSA-approved MVS meets the requirements of Federal Specification AA-V-2737 for storage of all levels of classified information and materials. A GSA-approved MVS must be six (6) sided (floor, ceiling, and four sides) and utilize a GSA-approved vault door. The door combination lock must conform to the Underwriters' Laboratories, Inc., Standard No. 768, for Group 1R or Group 1. An approved MVS is equivalent to a Class A vault and is suitable for SCIF construction.

a. Some advantages of modular vaults over conventional concrete vaults are:

(1) Portability of the system.

(2) Modular vaults have larger interiors than conventional vaults with the same exterior dimensions. Modular vault walls are not as thick as the conventional vault walls.

(3) Assembly/disassembly without degradation of vault panels and security.

(4) MVS takes less time to assemble and become operational.

(5) Minimal demolition/reconstruction of the structure or space that houses the vault.

(6) The basic MVS design allows for future expansion.

(7) Weight per unit area of the footprint of a modular vault can be as much as 84 percent less than that of a conventional concrete vault; some modular vaults could be located on upper floors in buildings.

b. The primary disadvantage of a MVS may be the initial cost for the system.

2. **GSA-Approved MVSs**: Two commercially available MVS have been tested and approved by GSA and are listed on qualified products list QPL-AA-V-2737. Factors to consider when selecting MVS include:

a. Volume of items to be stored.

b. Volume and size of items to be stored.

c. Size of housing structure.

d. Weight-supporting capacity of the housing structure.

e. Available accessories.

f. Purchase price, shipping expense, and assembly costs.

3. Manufacturer contact information:

Mosler
8133 Leesburg Pike, Suite 410
Vienna VA 22182
(800) 568-7233
(703)761-4669 (fax no.)

Hamilton
3143 Production Drive
Fairfield OH 45014
(513) 874-3733
(513) 874-3967 (fax no.)

ANNEX O

CONSTRUCTION SPECIFICATIONS FOR FIXED COMSEC FACILITIES

1. **Purpose**: To prescribe minimum construction requirements for fixed COMSEC facilities.

2. **Construction Requirements**: A fixed COMSEC facility must be constructed of solid, strong materials that will deter and detect unauthorized penetration. It must provide adequate attenuation of internal sounds that would divulge classified information through walls, doors, windows, ceilings, air vents, and ducts.

3. **Walls, Floors, and Ceilings**: Walls, floors, and ceilings shall be of sufficient structural strength to prevent or reveal any attempts at unauthorized penetration.

a. Walls shall be constructed from true floor to true ceiling.

b. Ceilings shall be at least as thick as the outer walls and offer the same level of security as the outer walls.

c. Where false ceilings are used, additional safeguards are required to resist unauthorized entry (e.g., installation of an approved intrusion detection system (IDS) in the area above the false ceiling). See Paragraph 6.b (note) for additional information.

4. **Doors and Entrance Areas**: Only one door shall be used for regular entrance to the facility. Other doors may exist for emergency exit and for entry or removal of bulky items.

a. All doors shall remain closed during facility operations and should only be opened to admit authorized personnel or material.

b. The following standards apply to facility doors and entrance areas:

(1) **Main entrance door**:

(a) Design and Installation: The access door must be of sufficient strength to resist forceful entry. The following types are allowed:

1. GSA-approved vault doors,

2. Standard 1-3/4 inch, internally reinforced, hollow metal industrial doors, **or**

3. Metal-clad or solid hardwood doors with a minimum thickness of 1-3/4 inch.

(b) The doorframe 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.

(c) The door shall be installed to resist the removal of hinge pins. This can be accomplished by either installing the door so that the hinge pins are located inside the facility or by set screwing/welding the pins in place.

(2) **Door lock**: The main entrance door to facilities which are not continuously manned must be equipped with a GSA-approved electro-mechanical lock meeting Federal Specification FF-L-2740.

(a) For facilities which are continuously manned, a built-in lock is not required; however, the door must be able to accommodate a GSA-approved electro-mechanical lock meeting Federal Specification FF-L-2740 and dead bolt should it ever become necessary to lock the facility from the outside (e.g., in case of emergency evacuation).

(b) An electronically activated 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 operationally manned. However, these locks do not afford the required degree of protection and may not be used to secure the facility when it is not manned.

NOTE: Facilities equipped with a GSA-approved, built-in Group 1R lock prior to 01 July 1993 may continue to use the Group 1R lock.

(3) **Other doors**: Other doors (e.g., emergency exit doors and doors to loading docks) must meet the same installation requirements as the main facility entrance doors and must be designed so that they can only be opened from inside 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.

NOTE: Approved panic hardware and locking devices lock bars, dead bolts, knobs, or handles) may be placed only on the interior surfaces of other doors to the facility.

(4) **Entrance areas**: The facility entrance area shall be equipped with a device which affords personnel desiring admittance the ability to notify personnel within the facility of their presence.

(a) Positive visual identification of a visitor must be established before entrance is granted.

(b) The entrance area shall be designed in such a manner that an individual cannot observe classified activities until cleared for access into the restricted spaces.

5. **Windows**: COMSEC facilities should not normally contain windows. Where windows exist, they shall be secured in a permanent manner to prevent them from being opened. The protection provided to the windows need be no stronger than the strength of the contiguous walls.

a. Windows that are 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 windows, shall 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 sealing them or equipping them on the inside with a locking mechanism.

b. Observation of internal operations of the facility shall be denied to outside viewing by covering the windows from the inside or otherwise screening the secure area from external viewing.

6. **Other openings**: Air vents, ducts, or any similar openings, which breach the walls, floor, or ceiling of the facility shall be appropriately secured to prevent penetration.

a. Openings, which are less than 96 square inches, shall have approved baffles installed to prevent an audio or acoustical hazard.

b. If the opening exceeds 96 square inches, acoustical baffles shall be supplemented by either hardened steel bars or an approved intrusion detection system (IDS).

> **NOTE: National policy and related criteria for acoustical control and can be found in IC Tech Spec for ICD/ICS 705 (Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities).**

ANNEX P

“SPECIAL” PHYSICAL SECURITY SAFEGUARDS FOR DOD BLACK BULK FACILITIES

1. **Purpose:**

a. To delineate the physical security safeguards that are unique to those facilities operated by or for the DoD, and employ classified crypto-equipment to protect multi-channel trunks passing encrypted or unclassified information, and otherwise referred to as DoD bulk facilities.

b. The area within a structure occupied by a DoD Bulk facility is referred to as a "space," and it is this "space" that requires the safeguards prescribed in this Annex. The structure, which contains the space is referred to as a "site."

2. **Construction Requirements:**

a. **Walls**: At sites which are not continuously manned, walls shall be of solid construction from true floor to true ceiling and shall be constructed in such a manner that attempts at unauthorized penetration will be detected or prevented.

b. **Doors**: Only one door should be used for regular entrance to the facility. The door must be strong enough to resist forceful entry. At sites that are not continuously manned, the entrance door shall be of substantial material (e.g., metal clad or solid wood with a minimum thickness of 1 and 3/4-inch, hinged from inside, fitted with a GSA approved electromechanical lock meeting Federal Specification FF-L-2740).

NOTE: Sites fitted with GSA-approved, built-in Group 1R locks with dead bolt extensions, or a heavy duty hasp and GSA-approved padlock prior to 01 July 1993 do not have to retrofit with electro-mechanical locks meeting Federal Specification FF-L-2740.

(1) Other doors may exist for emergency exits and moving bulky items. The doors must meet the construction criteria of the main entrance door and must be designed to open from inside the facility only. Approved panic hardware, intrusion detection, and locking devices (e.g., 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 bypass 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.

(2) A built-in lock is not required for sites continuously manned; however, the main entrance door must be able to accommodate a combination electromechanical lock meeting Federal Specification FF-L-2740 and dead bolt should it ever become necessary to lock the facility from the outside.

c. **Windows**: Where windows exist affording visual surveillance of personnel, documents, materials, or activities within the site, the windows 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 must be protected from forced entry. All perimeter windows at ground level, less than 18 feet above the ground, shall be covered by IDS.

d. **Access Control**

(1) During duty hours, the site entrance shall be under visual control at all times to preclude entry by unauthorized personnel. This may be accomplished by several methods (e.g. employee work station, guard, CCTV). Regardless of the method utilized, an access control system shall be used on the site entrance. An appropriately cleared person who is familiar with security procedures shall continuously escort persons not appropriately cleared within the space. Authorized personnel who permit another individual to enter the space are responsible for confirming the individual's access and need-to-know.

(2) An automated access control system may be used to control admittance to the site during working hours in lieu of visual control if it meets the criteria stated below.

(a) The automated access control system must identify an individual and authenticate that person's authority to enter the space through the use of an identification (ID) badge or card, or by personal identity verification. The ID badge or card must use embedded sensors, integrated circuits, magnetic stripes or other means of encoding data that identifies the site and the individual to whom the card is issued.

(b) In conjunction with the ID badge or card above, a personal identification number (PIN) is required. The PIN must be separately entered into the system by each individual using a keypad device and consist of four or more digits, randomly selected, with no logical association with the individual. The PIN must be changed when it is believed to have been compromised or subjected to compromise.

(c) Personal identity verification (Biometrics Device) identifies the individual requesting access by some unique characteristics such as: fingerprinting, hand geometry, handwriting, retina, or voice recognition.

NOTE: A procedure must be established for removal of the individual's authorization to enter the site/space upon reassignment, transfer or termination, or when the individual's access is suspended, revoked, or downgraded to a level lower than required.

e. **Daily Security Checks**

(1) In a continuously manned site, 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.

(2) In a site not continuously manned, the security check shall be conducted prior to departure of the last person. The check should ensure all COMSEC material is properly stored, that security containers are properly secured, and the space is secured against unauthorized access. The last person to depart shall ensure the entrance door to the site is locked and intrusion detection systems are activated. Daily security checks will be documented on a SF-701. Completed SF-701s will be retained in accordance with Annex T.

f. **Intrusion Detection System (IDS)**:

(1) Sites, that are not continuously manned, shall be equipped with an approved IDS. Either U.S. or Allied personnel may be assigned to monitor the IDS and to direct the responding guard(s). IDS must detect an attempted or actual human entry into the protected area. IDSs complement other physical security measures and consist of three essential components: intrusion detection equipment, security and response force personnel, operation procedures. Details of installed IDS shall be controlled and restricted on a need-to-know basis.

(a) Intrusion Detection Equipment (IDE). Primary power for all IDE will be commercial AC or DC power. 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.

(b) Alarm Condition Response. Every alarm condition will be treated initially as a detected intrusion until resolved by the response force. The response force will investigate the source of an alarm (e.g. intrusion, tampering, component or system power failure) and will notify site personnel. The response force will take appropriate steps to safeguard the site and prevent the escape of an intruder from the site as permitted by SOP, local law enforcement, and circumstances until properly relieved. Tests of the response force must be conducted semiannually. Results of investigations by the response force will be maintained at the monitor station.

(c) Operating Procedures. A written support agreement must be established for external monitoring and/or response.

(2) IDS sensors will be tested semiannually. The IDS will incorporate a means for providing historical record of all events, either automatically or through the use of a manual log system. If the IDE does not have a provision for automatic entry into an archive, the operator will record the time, source, and type of alarm, and action taken. The historical record must be routinely reviewed and retained by the command security officer. Records of alarm annunciation shall be retained for at least 90 days from the date of the alarm annunciation or until investigations of system violations and incidents have been successfully resolved and recorded.

ANNEX Q

GENERATING STATION OTAR AND OTAT LOG

The form on the reverse side of this page is for use in recording monthly OTAR/OTAT transactions. **Local reproduction of this form is authorized.**

Block Completion is identified, as follows:

1. **KEY SOURCE**

2. **SHORT TITLE**

3. **CLASS** (Classification of material sent/received)

4. **CONAUTH** (Controlling Authority of material sent/received)

5. **EFF PD** (Effective Period of material)

6. **STORAGE POSITION AND FILL DEVICE SERIAL Number (No.)**

7. **CIRCUIT** Identification **(I.D.) TRANSMITTED OVER RECEIVED** (Identify circuit used to transmit or receive)

8. **DATE/TIME OF TRANSMISSION**

9. **RECEIVING STATION(S)**

10. **ZEROIZED DATE/TIME**

11. **INITIALS** (Initials of the **two** personnel that **zeroized** the transaction)

CONFIDENTIAL (When filled In)

GENERATING STATION OTAR/OTAT LOG FOR THE MONTH OF: ______________________

1. KEY SOURCE	2. SHORT TITLE	3. CLASS	4. CON AUTH	5. EFF PD	6. STORAGE POSITION AND FILL DEVICE	7. CIRCUIT ID TRANSMITTED OVER RECEIVED	8. DATE/TIME OF TRANSMISSION	9. RECEIVING STATION(S)	10. ZEROIZED DATE/TIME	11. INITIALS

PAGE____OF____

CONFIDENTIAL (When Filled In)

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

ANNEX R

RELAYING/RECEIVING STATION OTAT LOG

The form on the reverse side of this page is for your use to record monthly OTAT transactions. **Local reproduction of this form is authorized.**

Block Completion is identified, as follows:

1. **KEY** Identification **(I.D.) SHORT TITLE**

2. **CONAUTH** (Controlling Authority of material sent/received)

2. **CLASS** (Classification of material sent/received)

3. **EFF PD** (Effective Period of material)

4. **DATE/TIME RECEIPT(R) TRANSMISSION(T)** (Identify date/time and annotate "R" for material received; "T" for material transmitted)

5. **CIRCUIT** Identification **(I.D.) TRANSMITTED OVER RECEIVED** (Identify circuit used to transmit or receive)

6. **STORAGE POSITION AND FILL DEVICE SERIAL** Number **(No.)**

7. **ZEROIZED DATE/TIME**

8. **INITIALS** (Initials of the **two** personnel that **zeroized** the key)

CONFIDENTIAL (When Filled In)

RELAYING/RECEIVING STATION OTAR / OTAT LOG FOR THE MONTH OF:______________________

1.KEY ID SHORT TITLE	2. CON AUTH	3. CLASS	3. CIRCUIT KEY INTENDED FOR	4 EFF PD	5. DATE/TIME RECEIPT(R) TRANSMISSION (T)	6. CIRCUIT I.D. TRANSMITTED OVER RECEIVED	7. STORAGE POSITION AND FILL DEVICE SERIAL NO	8. ZEROIZED DATE/TIME	9. INITIALS

PAGE_____OF_____

CONFIDENTIAL (When Filled In)

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

ANNEX S

COMSEC POINT OF CONTACT (POC) LISTING

* *

NAVAL COMSEC MATERIAL SYSTEM (NCMS/PMHS)

FACSIMILE:	Secure:	Non-Secure:
	COMM: (240) 857-7706	COMM: (240) 857-7715/7806
	DSN: 857-7706	DSN: 857-7715/7806

MESSAGE ADDRESS: NCMS WASHINGTON DC. Internal Office Codes:

00 - CO
01 - XO
N1 - Administrative
N3 – Operations (Includes Accounting, Equipment and Key Management)
N5 – Information Assurance (IA), Plans, Policies and Procedures
N6 – Public Key Infrastructure
N7 – Education and Training

NCMS (SIPRNET) Collaboration At-Sea (CAS)Website:

http://www.uar.cas.navy.smil.mil/secret/navy/39/site.nsf

MAILING ADDRESS: Naval Communications Security
Material System

ATTN (--)
1560 Colorado Ave,
Andrews AFB, MD 20762-6108

PRIMARY PHONE NUMBER(S):

DSN: 857-XXXX; COMM: (240) 857-XXXX

CO/XO - 9403

N3 - 7499 (Accounting)
- 8282 (Equipment/N3A)
- 1706 (LCMS)
- 7499/7808 (Key Div)
- 240-857-9787 (Vault)

N5 - 9831/3348 (Policy and Procedures)
- 7704/7708/7709: COMSEC Incidents, PDSs, Waivers and other policy matters)

N6 - 9735/9865/9401 PKI (Local Registration Authority, Mobile Training, Audits)

N7 - 7712/7815 (EKMS/KMI Audits, Training Visits, TDSP

COMMAND DUTY OFFICER - In the event you need immediate assistance (i.e., the issue **can not** wait to be resolved during normal working hours), contact the NCMS CDO at:

DSN: N/A COMM: (202) 345-3495

*** ***

COMSEC MATERIAL ISSUING OFFICE (CMIO) (PMHS):

DSN: 565-7051/53 COMM: (757) 444-7051/53

FACSIMILE: Secure: Same as above

Non-Secure:
DSN: 565-1745
COMM: (757) 445-1745

MESSAGE ADDRESS: CMIO NORFOLK VA//See note below//

NOTE: Office codes for message traffic:

N00 - OIC
N1 – Administrative
N3 – Distribution/Allowance
N35 – Vault Officer/Supervisor

MAILING ADDRESS:

OIC
CMIO Norfolk
8876 2nd Street
Norfolk, VA 23511-3797

*** ***

COR AUDIT TEAMS
ATLANTIC AREA

WASHINGTON DC

DSN: 764-2837 COMM: (202) 764-2837

E-MAIL: ncms_nafw_a&a_admin@navy.mil

GROTON CT

DSN: 694-3414 COMM: (860) 694-3414
E-MAIL: ncms_det_groton@navy.mil

NORFOLK VA

DSN: 646-9220/9221/9222/9223/9224 COMM: (757) 443-9220/9221/9222/9223/9224
E-MAIL: nrfk_cmsaa@navy.mil

MAYPORT FL

DSN: 960-6106 COMM: (904) 270-6106
E-MAIL: cmsaamayport@nctsjax.navy.mil

CAMP LEJUENE NC

DSN: 751-8204/8256 COMM: (910) 451-8204/8256
E-MAIL: cmsaa@usmc.mil

EUROPEAN AREA

NAPLES IT

DSN: 314-626-6142/3738 COMM: 011-39-081-568-6142/3738
E-MAIL: cmsaaeurcent@naples.navy.mil

PACIFIC AREA

FAR EAST FE

DSN: 315-243-6037/9216 COMM: 011-81-468-21-6037/9140
E-MAIL: cmsaafe@fe.navy.mil

PEARL HARBOR HI

DSN: 315-472-8881 ext 374 COMM: (808) 472-8881 ext. 374
E-MAIL: cmsaaph@navy.mil

PUGET SOUND WA

DSN: 744-6154 COMM: (360) 396-6154
E-MAIL: cmsaaps@navy.mil

SAN DIEGO CA

DSN: 526-2375/2377/2379 COMM: (619) 556-2375/2377/2379
E-MAIL: cmsaasd@navy.mil

* *

NSA AND MILITARY CENTRAL OFFICE OF RECORD (CORs)

NSA FILM DESTRUCTION FACILITY

FILM DESTRUCTION FACILITY: Used for the destruction of removable media (floppy disks).

MAILING ADDRESS:
Director National Security Agency
ATTN S174/Acct 889999
9800 Savage Road
Fort George G Meade, MD 20755-6000

DCS ADDRESS:
449563-BA21
FILM DESTRUCTION

NSA COR (TIER 0)

MESSAGE ADDRESS: DIRNSA FT GEORGE G MEADE MD//7131//

MAILING ADDRESS:
ATTN I513
National Security Agency
9800 Savage Road
Fort Meade, MD 20755-6000

PT1S FT HUACHUCA AZ

MESSAGE ADDRESS: CSLA TIER1

PHONE NUMBERS/OPERATIONAL POCs:

Tier 1:	DSN: 879-8238	COMM: (520) 538-8238
Tier 2/Tier 3:	DSN: 969-2557	COMM: (same as Tier 1 above)

MAILING ADDRESS:
Director, U.S. Army Communications
Electronics Command
Communications Security Logistics Activity
ATTN SELCL-ID-TIER1
Ft. Huachuca, AZ 85613-7090

PT1S SAN ANTONIO TX

MESSAGE ADDRESS: DIR TIER1 SAN ANTONIO TX

PHONE NUMBERS/OPERATIONAL POCs:

DSN: 945-1789/2567/2005 COMM: (210) 925-1789/2567/2005

MAILING ADDRESS: CPSG/DIWKM
230 Hall Blvd Suite 208, 209
San Antonio, TX 78243-7081

* *

MISCELLANEOUS POINTS OF CONTACT (POC)

DIRNSA INSECURITY

MESSAGE ADDRESS: DIRNSA FT GEORGE G MEADE MD//I9121//

ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS) CENTRAL FACILITY (CF)

STE REKEY: DSN: 936-1810 COMM: (410) 526-3200

Toll-FREE within CONUS/Canada: 1-800-635-6301
COMM: (410) 526-3208
DSN: 238-4600
URL: WWW.IAD.GOV/KEYSUPPORT

NOTE: For additional EKMS CF rekey/conversion telephone numbers, see paragraph 9 to Annex AD.

INTERNATIONAL HELP DESK (TECHNICAL ASSISTANCE CENTER (TAC)):

United Kingdom:	0800960403
Japan:	00531113346
Germany:	08008169780
Korea:	00798113210828
Italy:	800871340

USER ASSISTANCE:

Toll-FREE within CONUS: 1-800-635-5689
COMM: (410) 526-3208
DSN: 238-4600

MAILING ADDRESS: EKMS
P O Box 718
Finksburg, MD 21048-0718

MESSAGE ADDRESS: DIRNSA FT GEORGE G MEADE MD//______//

FACSIMILE:

	Secure:	Non-Secure:
DSN:	238-4108/27	238-4172
COMM:	(410) 526-3108/37	(410) 526-3172

QUESTIONS RELATED TO TERMINAL DELIVERIES, APPLICATIONS, ETC:

Phone:	COMM:	(410) 854-1711
	DSN:	244-1711

WEBSITE: https://www.iad.gov/securephone/index.cfm
Email: securephone@nsa.gov

STE	Secure FAX:	(410) 526-3127
	DSN	238-4127

COMMANDER, U.S. FLEET FORCES COMMAND (COMUSFLTFORCOM)

MESSAGE PLA: COMUSFLTFORCOM NORFOLK VA//N023EKMS//

PHONE NUMBERS:	DSN: 836-5853	COMM: (757) 836-5853
SECURE FAX:	DSN: 836-6497	COMM: (757) 836-6497
NON SECURE FAX:	DSN: 836-4118	COMM: (757) 836-4118

COMMANDER, U.S. PACIFIC FLEET (COMPACFLT)

MESSAGE PLA: COMPACFLT PEARL HARBOR HI//N633//

PHONE NUMBERS: COMM: (808) 471-8648

SECURE FAX/NON SECURE: (808) 471-4105

SPAWARSYSCEN ATLANTIC CHARLESTON SC

SPAWARSYSCEN ATLANTIC Charleston combines the services of the present Information Security (INFOSEC) support line with those of the Electronic Key Management System (EKMS) support line. This support line is available 24 hours a day and support personnel are physically available at a minimum of twelve hours per day, Monday through Friday.

NAVY EKMS TECHNICAL SUPPORT CENTER: TOLL FREE: 1-877-NAV-EKMS (628-3567)

NON-SECURE FAX: COMM: (757) 366-4700

SECURE FAX: COMM: (757) 366-4772

E-MAIL: NAVEKMS@SPAWAR.NAVY.MIL

MESSAGE ADDRESS: SPAWARSYSCEN ATLANTIC CHARLESTON SC //721SR//

MAILING ADDRESS: Commanding Officer
SPAWARSYSCEN ATLANTIC (Code 752)
P.O. Box 190022
North Charleston, SC 29419-9022

NAVAL FLEET TRAINING CENTER (NORFOLK VA)

MESSAGE ADDRESS: FLEETRACEN NORFOLK VA//C2M2//

MAILING ADDRESS: Commanding Officer
Fleet Training Center
9549 Bainbridge Ave
ATTN: EKMS COI
Norfolk, VA 23511-9549

PHONE NUMBERS: DSN: 564-1262 (Ext. 3030), COMM: (757) 444-1262 (Ext. 3030)

COAST GUARD, C4IT SERVICE CENTER (C4ITSC-BOD-IAB)

MESSAGE ADDRESS: COGARD C4ITSC ALEXANDRIA VA //BOD-IAB//
MAILING ADDRESS: Director C4IT Service Center
7323 Telegraph Road Stop 7340
Alexandria, VA 20598-7340

FACSIMILE: Secure: 703-313-5639 Non-Secure: 703-313-5640

PRIMARY PHONE NUMBERS:

Section Chief/Policy	703-313-5630
(SERVAUTH/CAA/CMD AUTH/CG ISIC)	703-313-5630
COMSEC Equipment/STE	703-313-5637
EKMS/KMI Action Officer	703-313-5632
KEYMAT Management Ops	703-313-5642
TEMPEST PM/CTTA	703-313-5631
AFTER HOURS**	703-303-5400

****CONTACT THE OOD AND REQUEST THE OOD CONTACT THE C4ITSC BEEPER****

COMMANDANT U.S. MARINE CORPS

MESSAGE ADDRESS: CMC C FOUR CY WASHINGTON DC//

MAILING ADDRESS: COMMANDANT U.S. Marine Corps (C4 CY)
Headquarters, U.S. Marine Corps
3000 Marine Corps, Pentagon
Washington, DC 20350-3000

PHONE NUMBER: DSN 223-3490 COMM: (703) 693-3490

FACSIMILE: Non-Secure
DSN: 223-3580 COMM: (703) 693-3560

JOINT COMSEC MANAGEMENT OFFICE

PHONE NUMBER: DSN: 968-2461
COMM: (813) 828-2461

FAX NUMBER: NON-SECURE DSN: 968-5293
SECURE DSN: 968-4250

MESSAGE ADDRESS: JCMO MACDILL AFB FL

MAILING ADDRESS: JOINT COMSEC MANAGEMENT OFFICE
8532 Marina Bay Drive
MACDILL AFB, FL 33621

STATUS INFORMATION:
HTTPS://VELA.STRATCOM.SMIL.MIL/RESTRICT/JCMO

SECAN WASHINGTON DC

PHONE NUMBER: IVSN: 514-1201
COMM: (443) 479-2868

MESSAGE ADDRESS: SECAN WASHINGTON DC

ANNEX T

RETENTION PERIODS FOR COMSEC FILES, RECORDS, AND LOGS

1. **Purpose**. To prescribe the minimum retention periods for COMSEC-related files, logs, and records (both active and inactive) used in COMSEC account management.

2. **Retention Periods**. The retention periods contained herein constitute **minimum** requirements for DON activities. Local policy may require longer retention periods. The destruction of inactive files, records, and logs should be accomplished as soon as practical after the minimum retention period.

a. **SF-153 LOCAL CUSTODY DOCUMENTS**. Retain for 2 years after the material has been destroyed or turned in to the EKMS Manager.

b. **LETTERS OF AGREEMENT**. Retain for 1 year after COMSEC support has been terminated.

c. **APPOINTMENT LETTERS**. Retain for 2 years from the date an individual has been relieved of his/her duties.

d. **ACCOUNTABLE ITEM (A/I) SUMMARY**. Destroy when replaced with an updated version.

e. **LCMS AUDIT DATA**. Retain audit data until the next COR audit. Data such as signatures and credentials must be deleted when no longer effective.

f. Audit Review Logs for **Electronic Storage Devices that possess audit capability (DTD, SDS, SKL, TKL)**. Retain for 2 years (Unless a longer duration is stipulated in local command policy. Retention of the audit trail itself is only required when anomalies are detected that require further review.

g. **ARCHIVED DATA**. Regardless of platform configuration (Phase 4, 5, etc…) LCMS archived data(e.g., accounting records) will be retained for 4 years.

h. **INVENTORY REPORTS.** Both working copies generated for inventorying material at the local account level and each local element, as well as consolidated inventory reports will be retained in the Chronological File for 2 years (**current year plus previous 2 full years)**.

i. **WATCH-TO-WATCH INVENTORY SHEETS**. Retain for 30 days beyond last recorded inventory date on the sheet.

j. **VISITOR REGISTER**. Retain for 1 year from the date the register has been completed or closed out.

k. **TRANSACTION STATUS LOG**. Maintain copies as specified below:

TYPE COMMAND	**FREQUENCY OF PRINTOUTS**	**RETENTION PERIOD**
Submarine	Prior to deployment	Destroy when Replaced with updated versions
Surface or Deployed Mobile Units	Once a month	Destroy when replaced with updated versions
Shore or Non Deployed Mobile Units	Once every 3 months	Destroy when replaced with updated versions

NOTE: Each account will close out their Transaction Status Log at the end of each calendar year and retain it on file for 2 years (**current year plus 2 full years**).

l. **RECEIPT, TRANSFER, GENERATION, POSSESSION, CONVERSION, RELIEF FROM ACCOUNTABILITY (i.e., SF-153 REPORTS) and KEYING MATERIAL SUPERSESSION NOTICES.** Retain for 2 years (current year plus previous 2 years).

NOTE: Chronological files will be grouped together at the end of each calendar year and labeled with their authorized date for destruction. Example: 2007 Chronological files are authorized for destruction 1 Jan 2010, 2008 Chronological files are authorized for destruction 1 Jan 2011, etc…

m. **DESTRUCTION RECORDS** (e.g., SF-153, CMS 25 (or equivalent form used to record destruction) SF-153). The following pertains:

(1) Retain Consolidated destruction reports for 2 years (**current year plus previous 2 full years**) for SECRET and above.

(2) **Effective with AMD-7,** retain local destruction reports (e.g. SF-153, CMS 25) for 2 years (**current plus previous 2 full years.** CMS-25s used to document destruction of segmented physical material will be turned in with the SF-153 (working copy) of the destruction report provided by the Manager or created manually.

(3) Documentation and retention for CONFIDENTIAL and below material assigned ALC 4 and 7 material is at the discretion of the CO/OIC since there is no prescribed requirement to document destruction of CONFIDENTIAL and below material assigned ALC 4 or 7.

NOTE: Effective with AMD-7, upon verification of all information including dates and signature data reflected on local destruction documents (CMS-25s and SF-153s), EKMS Managers will retain the working copies of the destruction reports with the corresponding CMS-25s attached to them for 2 full years (current year plus last (2) full calendar years.

n. **CORRESPONDENCE and MESSAGES**.

(1) Retain COMSEC-related GENERAL messages authorized for destruction by the originator or as reflected on the next year’s annual recap message, as applicable.

(2) Retain general correspondence and all other messages relating to only account holdings for 2 years.

o. **DIRECTIVES and INSTRUCTIONS**. Retain required items related to your account until cancelled or superseded.

p. **OTHER RECEIPTS.** (i.e., DCS, registered mail). Retain for 1 year.

q. **COMSEC FACILITY INSPECTION**. All required inspections must be documented and records kept on file at the facility and the cognizant security officer for 3 years.

r. **Navy EKMS ST&E CERTIFICATION MESSAGE**: Retain until no longer valid.

s. **OTAR/OTAT**: Commands generating, sending, receiving, and relaying electronic key for OTAD/OTAR/OTAT must retain local accounting records for a minimum of 60 days following the date of the last entry on the key generation log. This retention requirement applies to both field-generated key and key converted from tape key.

t. **Key Conversion Notice (KCN)**: Retain for 2 years.

u. **LMD/KP Pin/CIK Log:** Retain for 2 years following the date of the last recorded Log entry.

v. **Fill Device (FD) label (yellow card):** Retain for 90 days after final zeroization of the key or until destruction is verified through receipt/verification of a Key Conversion Notice.

w. **Spot Checks/Semi-Annual Assessments:** Completed spot checks and/or semi-annual assessments will be retained for 2 years or until completion of the next COR Audit (if waived and not conducted within 2 years)

x. **COR Audit Reports:** Will be retained until the following audit and receipt of the report for the later audit.

y. **Completed SF-701/SF-702s**: Will be retained for 30 days beyond the last date recorded on them in accordance with SECNAV M5510.36(series).

z. **EKMS CF Notices**: Retain for 2 years.

aa. **Messages, letters or memorandums used to document and/or report COMSEC Incidents or PDSs**: Retain for 2 years.

ab. **SD Form 572**: Retain for 90 days from the date the individual is relieved of their responsibilities involving COMSEC material.

ac. **Training**: Training Reports for training scheduled and completed by LEs, including that facilitated by EKMS Managers, Alternates or LE Issuing (such as stand downs or EAP/EDP drills conducted) will be retained for 2 years.

ad. **CF User Registration Data:** Retain a printed copy in the chronological file until modified and a later version is received from the CF.

ae. **CF Key Orders**: Retain on file for two years.

af. **Access Lists**: Retain for 90 days when updated.

ag. **SKL/DTD/TKL Reinitialization Verification**: **Effective with AMD-7,** documentation must exist to provide the means to verify the device(s) are reinitialized annually. This can be achieved through uploading and printing the audit trail immediately after initializing or reinitializing the device(s) or through the addition of a column on the accounts exists Audit Trail Review Log. Such documentation will be retained for 2 full years. See Annexes Z and AF Paragraphs 6.B.1.A or 7.A.5, as applicable for additional information.

ah. **EKMS Manager Turnover Checklist:** Effective with AMD-8, attach to Change of EKMS Manager Inventory (CCIR) and retain in accordance with Annex T Paragraph 2.i.

ANNEX U

COMPLETING LOCALLY PREPARED SF-153 COMSEC MATERIAL ACCOUNTING REPORTS

1. **Purpose**: To provide guidance for completing SF-153 COMSEC material accounting reports.

2. **Preprinted SF-153 COMSEC Material Reports**:

a. There are currently many versions of the preprinted SF-153 COMSEC Material Report authorized for use.

b. All versions contain identical data blocks of information but are assigned unique transaction numbers when generated from LCMS.

c. The example SF-153 and amplifying data contained in this Annex, as well as those generated from LCMS conform to revision 12-96.

3. **Locally Prepared SF-153s**:

Locally prepared SF-153s must contain identical data blocks of information as identified in paragraph 8 below.

NOTE: The information that follows is provided to support the "manual" completion of COR-reportable SF-153s (e.g., in the event of catastrophic failure of the LMD/KP) and to assist LEs, who are not LCMS equipped, in completing local SF-153s.

4. **Verifying Completeness and Accuracy**:

a. The accuracy of accounting reports is an extremely important aspect of account management. Consequently, prior to forwarding a report, the completeness and accuracy of all information **must be** verified.

b. Incomplete/erroneous COR accounting reports (e.g. missing addresses, dates, transaction numbers, signatures or the report contains errors in the short title(s) or accounting data) forwarded to the COR cannot be processed until all errors are corrected.

c. Changes or corrections to a SF-153 COMSEC Material

Accounting Report must be reported to the COR via phoncon, message or facsimile.

5. **Assigning Transaction Numbers (TNs)**:

a. Transaction Numbers (TNs) maintain the continuity of COMSEC transactions and provide a means of verifying individual account records and are automatically assigned in LCMS.

b. TNs are composed of the account’s EKMS ID, date (YYMMDD), and the sequential number of the transaction. For example, if the EKMS ID number of the account is 078002, the current date is 19991203, and it is the first transaction, the TN would be 078002 19991203 1.

6. **Line Entries on SF-153 Accounting Reports**:

a. Material must be listed one item per line on all SF-153 Accounting Reports.(except as noted in 6.b and 6.c below.)

b. If multiple copies of an edition of an AL Code 1 short title are being reported and the accounting numbers are in consecutive order, one line entry should be used (e.g., USKAA 888 AB 344, 345, and 346 may be listed as: "USKAA 8888 AB 344-346.").

c. For AL Code 2 or 4 material (accountable by quantity), list multiple copies of the same short title and edition as a single consolidated line entry.

d. If accounting numbers are not in consecutive sequence (i.e. sequential number is broken), a separate line entry is required for each.

e. Different editions of the same short title must be listed separately.

f. Close-out Line Entries on Accounting Reports:

(1) Immediately below the last short title entry on the last (or only) page of an SF-153 Accounting Report, enter "TOTAL LINES: _______ TOTAL QUANTITY:_______" as a single line entry.

(2) The total lines entry is the total of all short title line entries.

(3) The total quantity entry is the total of the

quantity column for all short titles listed on the report.

7. **Signature Requirements**:

Department of the Navy (DON) Two Signature Receipt Policy. The intent of this policy is twofold: (1) to ensure incoming COMSEC material shipments to COMSEC Account commands are acknowledged by at least two account personnel, and (2) that the incoming shipments are handled expeditiously (opened and processed as soon as feasible). The two signatures merely serve to document receipt acknowledgement. Once the signatures are affixed, one person can proceed to open and process the shipment as long as the shipment does not contain material requiring TPI handling.

Except for DON Logistics Agency/Depot Accounts (e.g., CRFs, CMIO), the following receipt signature policy applies to all other DON COMSEC Accounts:

-- "Receipts" for incoming shipments of ***physical*** COMSEC material/equipment and CCI at the EKMS Manager Account Level must be signed by two authorized people, one of whom must be the EKMS Manager or Alternate. ***Physical*** in this context also includes receipt of electronic key(s) stored in data transfer devices or on removable media (e.g., floppy disk or CD) but does **NOT** include either of the following: (1) electronic keys (Bulk Encrypted Transactions/BETs) received directly to the LMD/KP desktop via x.400 delivery, (2) BETs received via SIPRNET and saved to a floppy diskette/CD for subsequent uploading to LMCS).

-- **Local Custody Document Signature Requirements**: See Article 712.d

a. Inventory, Relief from Accountability, Possession, Generation, and Hard Copy Consolidated Destruction Reports :

(1) Require the signature of the EKMS Managers and Alternate Manager or a properly cleared EKMS witness, as well as the CO/OIC/SCMSRO, as applicable (block 17).

(2) In the absence of Commanding Officer, the Executive Officer is authorized to sign accounting reports as "Acting" Commanding Officer. The use of By Direction is **not** authorized.

(3) Accounting reports that are signed by the SCMSRO must be annotated to reflect "Staff CMS Responsibility Officer" vice by direction or acting.

NOTES: 1. All Generation, Inventory, Possession, Relief from Accountability, and Consolidated Destruction reports require (3) signatures.

2. Missing applicable signatures on accounting reports constitutes a PDS in accordance with Article 1005.

b. **Reports listing SAS/TPC Material**:

(1) SF-153 Transfer and Destruction reports that list SAS/TPC material must be signed by two members of the SAS/TPC team.

(2) SAS/TPC accounting reports must be given to the EKMS Manager for use in reporting the transfer, destruction or receipt of SAS/TPC material to the COR (CJCSI 3260.01(series) contains basic accounting and control guidance for SAS/TPC material).

c. **Other Reports**:

(1) For Depot/Logistics accounts (CMIO, Crypto Repair Facilities/VGLS accounts): One signature is required from the Depot/Logistic account to process incoming shipments of COMSEC equipment provided keying material is not included in the shipment. If keying material is included in the shipment, two signatures are required from the Depot/Logistic account. The EKMS Manager or Alternate should provide the signature(s).

(2) Local destruction records require the signature of the two personnel who destroyed the material.

(3) Local inventory records require the signature of the two personnel who inventoried the material reflected.

NOTE: Parent account commands may require their "external LEs" to also include the signature of their CO/OIC/SCMSRO. Such additional signature requirements should be spelled out in the letter/memorandum of agreement (LOA/MOA) between the two commands.

d. All hardcopy accounting reports submitted to the COR must be the signed original.

e. Signatures generated by means of a signature stamp or other signature devices are not permitted.

f. A carbon copy or a reproduced copy of an original accounting report is acceptable for the following two purposes:

(1) Local record retention; and

(2) Receipt to the originator of a material transfer.

NOTE: Signatures on reproduced accounting reports must be clearly visible.

g. Signature Data. In addition to the written signature, the name, rank/rate/grade, and service of each person who signs an accounting report must be typed, printed, or stamped in the appropriate block(s) of the report.

8. **Completing Multi-Page SF-153 Reports**:

a. When a multi-page SF-153 is used, the closeout line information ("TOTAL LINES: TOTAL QUANTITY:") must be entered only on the last page (immediately below the last short title entry).

b. Blocks 1-6 on each page of a multi-page accounting report must be completed.

c. Only one TN may be assigned to a multi-page accounting report. Consequently, all material listed in the report is treated as a single transaction.

d. Annotate the consecutive page number in block 17 on each page of the report and record the total pages comprising the multi-page report on the last page (e.g., 10 of 10).

e. Signatures are required only on the **last page** of a multi-page report.

9. **Completing Data Blocks 1-17 of the SF-153**:

a. **Block 1- Type of Report**: Indicate the type of report by placing an "x" in the appropriate box. If the specific type of report being prepared is not listed, place an "x" in the box marked "Other". Next to this box, annotate/type the type of report (e.g., LCI).

b. **Block 2 – From**: Enter your account command title, complete mailing address, and EKMS account number.

NOTE: If a "Local" SF-153 Accounting Report (e.g., local destruction, local inventory) is being prepared, the EKMS account number may be omitted.

c. **Block 3 – Date of Report**: Enter the date as year, month, and day (e.g., 19990815). Complete Block 3 as indicated below for the following reports:

AMD-9

(1) Transfer reports: Completed by the originator of the transfer and ~~must~~ reflects the date that the report was ~~actually~~ prepared.

AMD-9

(2) Destruction reports: If date of destruction is different than the date the report was prepared, annotate the date of destruction in block 13 and have destruction personnel initial. ~~Completed by the originator and must reflect the date on which the material listed was actually destroyed.~~ If report is being used to consolidate other destruction records (e.g., from LEs), only the date of report preparation is necessary.

AMD-9

(3) Possession, Relief from Accountability, Conversion, and Inventory Reports: Completed by the originator and ~~must~~reflects the date the SF-153 is being ~~signed~~ prepared.

AMD-9

(4) Generation reports: Completed by the originator and ~~must~~ reflects the date that the report was ~~actually~~prepared.

d. **Block 4 – Outgoing TN**: Originator TN assigned from the EKMS Transaction Log.

e. **Block 5 – Date of Transaction**: For recipients of Transfer Reports, **Hand Receipts (LCI documents)** and originators of Generation Reports, enter the date the SF-153 is signed. Leave this block blank for Destruction, Transfer, Possession, Conversion, Inventory, and Relief from Accountability Reports.

f. **Block 6 – Incoming TN**: Recipient TN assigned from the EKMS Transaction Log.

g. **Block 7 – To**:

(1) For SF-153 Transfers: Enter the command identification, complete mailing address, and the EKMS account number of the unit to which the material is being sent. (**NOTE: When the intended recipient is a ship, include the type and hull number of the ship instead of geographic location.**)

(2) For SF-153s Used to Issue Material on Local Custody: Enter the command title or identification of LE.

(3) For SF-153 Possessions, Generation, Conversion ADD, and Inventories (Special) Reports: Enter the same data as entered in Block 2. (**NOTE: Blocks 2 and 7 must reflect the same information.**)

~~(4) For SF-153 Conversion DELETE and Relief from Accountability Reports: Enter: "CMS REMOVAL" and account number: 095999.~~

AMD-9

~~(5) For SF-153 Destructions: If preparing the report for submission to the COR, insert "CMS DESTRUCTION" and insert account number 095997. Otherwise, leave blank.~~

h. **Block 8 – Accounting Legend Codes**: Leave blank.

i. **Block 9 – Short Title/Designator-Edition**: Enter the short title(s) and accounting data for the applicable COMSEC material in accordance with Article 225.

(1) Block 9 close out line: Immediately below the last short title line entry, enter: "TOTAL LINES______TOTAL QUANTITY______."

(2) **Block 9 - Special Remarks**: Below the "TOTAL LINES/TOTAL QUANTITY" entry, the following remarks, though not all inclusive, should be entered as applicable:

(a) Destruction Reports: Annotate the destruction authorization (e.g., CONAUTH, originator and date-time-group of message).

(b) Transfer Reports: Cite transfer authorization in accordance with Article 733. Additionally, DON accounts must include the transfer statement in Article 733.a when transferring material to another service account or agency (e.g., Army, NSA).

j. **Block 10 – Quantity**: Enter the quantity of items reflected in Block 9.

k. **Block 11 – Accounting numbers (beginning/ending)**: Enter the accounting number(s) of the short title(s) listed in Block 9. If the quantity is one, the beginning column may be left blank and the accounting number entered in the ending column.

l. **Block 12 – AL Code**: Enter the AL Code of the short title.

m. **Block 13 – Remarks**: Enter any information considered pertinent to the report.

n. **Block 14 – Type of action taken**: Place an "x" in the appropriate box. If the type of action taken is not indicated, leave all boxes blank.

o. **Block 15 – Authorized recipient**:

(1) Blocks 15a and 15b: Signature of EKMS Manager and rank/grade for all reports, **less** transfers. (**NOTE: When completing multi-page reports, signatures are required only on the last page**.)

(2) Blocks 15c and 15d: Print the name of the EKMS Manager and or Alternate/EKMS Witness and branch of service, if applicable, using black or blue black pen.

p. **Block 16 – Witness**: Place an "x" in the box marked "Witness" when receipting for all COMSEC material (includes crypto equipment and CCIs) and for Possession (generated/submitted as the result of a Found Material COMSEC incident), Destruction, Inventory, Conversion, and all Relief from Accountability Reports.

(1) Blocks 16a and 16b: Signature of EKMS Witness and rank/grade for all required reports. (**NOTE: When completing multi-page reports, signatures are required only on the last page**.)

(2) Blocks 16c and 16d: Print the name of the EKMS Witness and branch of service, if applicable.

q. **Block 17 – Commanding Officer signature data**: The signature of the Commanding Officer, SCMSRO, or OIC, as applicable, is required only on Inventory, Relief from Accountability, Generation, Possession (generated/submitted as the result of a Found Material COMSEC incident), and Hard Copy Consolidated Destruction Reports. **On multi-page accounting reports, signatures are only required on the final page.**

NOTE: The CO's signature requirement for destruction reports is waived for all Naval Reserve Force EKMS accounts per NCMS policy waiver letter dated 26 Apr 94.

r. **Block 17 – Page number information**: Enter the appropriate page number information (e.g., Page 1 of 1).

10. Commonly used accounting reports and a brief description of each is reflected below. Additional accounting reports may be found in the EKMS-704 (series).

(1) Transfer Report Initiating (Type 13): Used to document and/or report the movement of COMSEC material from one EKMS account to another or from one LE to another LE (i.e., local custody issue).

(2) Destruction Report (Type 1): Used to document and/or report the destruction of COMSEC material.

(3) Possession Report (Type 9): Used to document and report possession of COMSEC material.

(4) Transfer Report Receipt All (Type 14): Used to document and/or report receipt of COMSEC material where an existing Transfer Report Initiating exists.

(5) Transfer Report Receipt Exception (Type 15): Used to exclude items from a Transfer Report Initiating that were not received.

(6) Transfer Report Receipt Individual (Type 16): Used to document and/or report receipt of COMSEC Material where no existing Transfer Report Initiating exists.

(7) Relief from Accountability Report (Type 11): Used for a variety of purposes where the originating account requires relief of accountability for COMSEC material assigned AL Code 1, 2, or 6. Uses are identified in Article 745.a.

(8) Conversion Report (Type 0): Used to document and report changes to short titles and/or accounting legend code data from the COR database and the entry of new data.

NOTE: Conversion Reports are submitted only when directed by the COR or NCMS.

(9) Request Inventory (Type 18): Used by the COR to trigger the inventory cycle process.

(10) Inventory Report (Type 6): Used to document and

report the physical inventory of COMSEC material.

(11) Inventory Reconciliation Status Transaction (IRST) (Type 17): Used to report the differences between the Tier 1 and Tier 2 databases.

(12) Generation Report (Type 5): Used to document the generation or import of key.

(13) Cancel Distribution (Type 10): Used to cancel a Transfer Report Initiating (TRI) or Issue Report Initiating and to document/report the cancellation.

ANNEX V

REPORTING PAGE CHECK OR OTHER DISCREPANCIES IN COMSEC MATERIAL/RELATED DEVICES AND CCI

1. **Purpose**: To prescribe actions required when discrepancies are noted during page checks or verification involving:

a. COMSEC keying material marked CRYPTO.

b. COMSEC manuals and publications.

c. Classified COMSEC equipments and related devices (includes CCIs).

2. **Using the Discrepancy Reporting Legend**:

a. The categories of COMSEC material that a discrepancy is applicable to are identified as follows:

K:	Keymat marked "CRYPTO".
CM/A:	Classified COMSEC-Related Manuals/Publications.
CA:	Classified Amendments.
UM/A:	Unclassified COMSEC-Related Manuals/Publications and Amendments
E:	Classified COMSEC Equipment (**not** designated CCI).
R:	Related Devices (**not** designated CCI).
CCI:	CCI Equipment and Related Devices

b. The above letters will appear in parentheses before each type of discrepancy in paragraph 3 below. Action required to address these discrepancies is outlined below the discrepancy.

3. **Discrepancies and Required Action**:

(K) Pages or segments discovered missing upon initial receipt page check.

Report IAW Chapter 9. If replacement material is required, the applicable COR must be an action addressee with information to NCMS WASHINGTON DC//N3// and CMIO//N3//.

NOTE: Do not page check keymat sealed in canisters.

Pages or segments discovered missing on occasions other than initial receipt page check.

Report IAW Chapter 9. If replacement material is required, the applicable COR must be an action addressee with information to NCMS WASHINGTON DC//N3// and CMIO//N3//.

(K) Duplicate pages or segments.

Retain duplicate pages or segments. Notify DIRNSA//I31132/I31//, INFO NCMS//N3// and Controlling Authority.

(K) Defective keying material.

Report defect to DIRNSA//I31132/I31//, INFO NCMS//N3//, CMIO//N3//, and Controlling Authority. Retain defective keying material until disposition instructions are received from DIRNSA. If replacement material is required, the applicable COR must be an action addressee with information to NCMS WASHINGTON DC//N3// and CMIO//N3//.

(K) Pages or segments misnumbered and/or out of sequence. Resequencing of pages is possible.
Report discrepancy to DIRNSA//I31132//, INFO NCMS//N3// and Controlling Authority. Re-sequence pages or segments.

(K) Pages or segments out of sequence. **NOT** possible to resequence pages.

Report discrepancy to DIRNSA//I31132//, INFO NCMS//N3//, CMIO//N3//, and Controlling Authority.

Retain defective keying material until disposition instructions are received from DIRNSA. If replacement is required, the applicable COR must be an action addressee with information to NCMS WASHINGTON DC//N3// and CMIO//N3//.

(CM/A) Pages discovered missing or misprinted upon initial receipt.

Report discrepancy to originator, INFO NCMS//N3// and CMIO //N3//. If replacement material is required, both NCMS and CMIO must be action addressees.

(CM/A) Pages discovered missing on occasions other than initial receipt page check.

Report IAW Chapter 9. If replacement material required, CMIO//N3// must be action and NCMS//N3// info addressee.

(CM/A) "Unclassified" pages discovered missing on occasions other than initial page check.

Report to NCMS//N3//, INFO CMIO//N3//. If replacement material required, NCMS//N3// and CMIO//N3// must be action addressees.

(CM/A) Page(s) duplicated.

Report discrepancy to originator, INFO NCMS//N3//. Retain page(s) and await disposition instructions.

(CM/A) Pages misnumbered and/or out of sequence; resequencing is possible.

Report discrepancy to originator, INFO NCMS// N3// and re-sequence pages.

(CM/A) Pages misnumbered and/or out of sequence; NOT possible to resequence.

Report discrepancy to originator, INFO NCMS//N3// and CMIO//N3//. If replacement material required, NCMS//N3// and CMIO//N3// must be action addressees. Retain defective material until disposition instructions are received from originator of material.

(CM/A) Technical data is incorrect or missing, or a preparation or format error is discovered.

Report discrepancy to originator, INFO NCMS//N3// and CMIO//N3//. Retain defective material until disposition instructions are received from originator of material.

(UM/A) All discrepancies.

Report IAW Chapter 10.

(E/R/CCI) Component(s) discovered missing upon initial receipt.

Report missing component(s) to NCMS//N3/N5//, INFO CMIO//N3// or originator of shipment. If replacement required, originator of shipment must be action addressee.

(E/R/CCI) Component(s) discovered missing when equipment/device checked on occasion other than initial receipt.

Report IAW Chapter 9. Request replacement component(s) IAW Chapter 6.

(E/R/CCI) Defective equipment/device.

Attempt to have qualified technician repair locally. If unable to repair locally, contact CRF. Marine Corps elements contact supporting Electronics Maintenance Support Company (ELMACO) or Force Logistics Support Cryptographic Facility (FLSCF)).

ANNEX W

MINIMUM PAGE CHECK REQUIREMENTS FOR COMSEC MATERIAL

THESE PAGE CHECK REQUIREMENTS DO NOT APPLY TO KEYING MATERIAL PACKAGED IN CANISTERS

TYPE OF MATERIAL	UPON INITIAL RECEIPT	AFTER ENTRY OF AMENDMENT WHICH CHANGES PAGES	UPON INSTALLATION/MODIFICATION	DURING EKMS ACCOUNT INVENTORIES	DURING WATCH INVENTORIES	PRIOR TO TRANSFER TO NEW ACCT	UPON DEST INVENTORIES
UNSEALED KEYING MATERIAL	YES	N/A	N/A	YES	YES	YES	YES
RESEALED KEYING MATERIAL	N/A	N/A	N/A	YES	N/A	YES	YES
CLASSIFIED COMSEC ACCOUNTABLE PUBLICATIONS (I.E. AKAA, AKAC, AKAI, KTC's,USKAC, USKTC)	YES EXCEPT AS INDICATED IN ART 757.E.3	YES	N/A	YES EXCEPT AS INDICATED IN ART 757.E.3	YES	YES	YES
UNSEALED MAINTENANCE AND OPERATING MANUALS	YES	YES BY PERSON ENTERING & BY PERSON VERIFYING ENTRY	N/A	YES EXCEPT AS INDICATED IN ART 757.E.3	N/A	YES	YES
ALL UNSEALED AMENDMENTS	YES	YES BY PERSON ENTERING & BY PERSON VERIFYING ENTRY	N/A	YES EXCEPT AS INDICATED IN ART 757.E.3	YES	YES	YES
UNSEALED AMENDMENT RESIDUE	N/A	YES BY PERSON ENTERING & BY PERSON VERIFYING ENTRY	N/A	N/A	N/A	N/A	YES
MAINTENANCE AND REPAIR (PWB OR Q) KITS	YES ALL COMPONENTS SEE NOTE 1	N/A	YES CLASSIFIED COMPONENTS ONLY	YES EXCEPT AS INDICATED IN ART 757.E.3 (CLASSIFIED COMPONENTS ONLY)	N/A	YES ALL COMPONENTS	YES
EQUIPMENT	YES UPON UNCRATING	N/A	N/A	YES	YES	YES	YES
MANDATORY MODIFICATION ON NSA/NAVY	YES	N/A	YES	YES MOD PLATE ONLY	N/A	YES	N/A

NOTE: MAINTENANCE PERSONNEL MUST INVENTORY ALL COMPONENTS UPON INITIAL LOCAL CUSTODY AND RECEIPT AND UPON RETURN OF REPAIR KITS. RESEALING KEYING MATERIAL INCLUDING ROB AND WHENDI MATERIAL TO AVOID PAGE CHECKS IS AUTHORIZED.

ANNEX X

EKMS SUITE

1. Suite Description

The LMD/KP suite must only be operated by authorized individuals who have been assigned key management responsibilities. The LMD must be disconnected when the associated STE is being used for NON-EKMS purposes. Remote dial-in access from another site is **prohibited.**

a. General: Minimum system requirements for the EKMS suite can be found in EKMS-704(series). Operational requirements will dictate suite configurations for individual commands. The following is provided as a general listing of EKMS suite components:

(1) a commercial off the shelf (COTS) CPU with a 101 key AT-style keyboard.
(2) serial mouse
(3) 17" SVGA color monitor
(4) KOK-22A key processor
(5) printer

b. LMD: The LMD (or CPU).

NOTE: Configuration management for the LMD is controlled by SPAWARSYSCEN (SSCN) ATLANTIC. Only CPUs procured by SSCN ATLANTIC specifically for this purpose may be used.

c. KP: EKMS-705A (KOK-22A Manual) is issued at time of installation; consult EKMS-705A for exact dimensions and capabilities. **NOTE:** There is no "OFF" switch for the KP, it is either "ON" or in "STANDBY". Operator maintenance is limited to resetting a circuit breaker that is located in the back of the unit. In addition to the ON/STBY indicator, the KP has three indicator lights on the front: alarm, battery low, and zeroized. The front panel also consists of the following: fill device port, LED display window, multi-function keypad, a zeroize button, and two CIK (KSD-64) ports. The back of the unit consists of connection ports, circuit breaker, and power supply connection.

NOTE: Due to the power requirements of the Key Processor and to prevent possible damage and/or failure of the KP, EKMS Managers will not connect the KP to an UPS unit. The

LMD however, will be supported by an UPS.

2. **BIOS Password**:

The Basic Input/Output System (BIOS) of the LMD will be password protected to prevent access and changing of the authorized configuration and boot options. The BIOS password will be configured by and retained by SSCN Atlantic. To ensure strict configuration management and the security of the LMD, mandated in National Doctrine, this password will not be made available to EKMS Managers at the Local Account/Tier 2 level.

3. LMD Boot Restrictions:

The LMD **MUST** boot from its hard disk (removable hard drive). Booting from floppy disk, CD, or tape is permissible only for initial installation, upgrades, and system maintenance.

4. **Powering Up the LMD**:

The following steps are provided in order to properly power up the LMD and are outlined in EKMS-704 series:

a. Power up KP, LMD and Monitor and verify that each item boots up properly. The normal start-up process will commence and take approximately 2-3 minutes for the proper boot sequence to complete. Follow the below procedure or refer to EKMS 704 (series) LMD/KP Operators Manual for further information.

(1) At the "**DOD Warning Banner**", depress the "**ENTER**" key.

(2) At the Login screen, type a valid username and password, then depress the "**ENTER**" key.

5. **Powering Down the LMD**:

In order to properly power down the LMD/KP, the following is provided:

(1) Log off the KP (as applicable) before attempting to log off the LMD.

(2) On the LCMS Menu, click on **Log Off.** On the pull-down menu, click on **Log Off LCMS.** In the pop-up window, click on **Continue**; this option will automatically log the LMD/KP Administrator/Operator off the KP as well. When prompted by the KP, remove Administrator/Operator CIK and depress "**ENTER**" on KP

keypad. Depress “**STBY**” button to place KP in standby mode.

(3) The black LCMS window is then displayed. When **Shutdown complete** is presented, at the **#** prompt (It may be necessary to depress “**Enter**” key after **Shutdown complete** is presented to get the **#** prompt), type:

clean and depress the “**Enter**” key.

At the subsequent prompt type:

dbshut and depress the “**Enter**” key.

A series of lines of information will then be presented with the last line saying **Database “a” shut down.**

(3) Using your mouse, move the pointer to the right hand side of the screen, hold down the left mouse button and the popup menu labeled **SCO Open Server Software,** scroll down to the label **System Shutdown**, then release the left mouse button.

(4) **Do not power off at this time.** Wait until you are presented with the following display:

**** Safe to Power Off ****
or
**** Press Any Key to Reboot ****

(5) At this time it is safe to power the system down.

The importance of following this procedure exactly, every time the system is shut down, cannot be overemphasized.

6. **Local Area Network (LAN) Restrictions**:

Connection of the LMD/KP to a Local Area Network (LAN) or remote login is **strictly prohibited** and is in violation of National and Naval Doctrine. The only authorized exception is through a Virtual Private Network (VPN).

7. **Software Restrictions**:

With the exception of NSA Authorized User Application Software (UAS) programs (e.g., Cardloader UAS (CLUAS), Common UAS (CUAS), etc…), **no software other than that installed during site initialization is authorized.** Additionally, all scripts, software upgrades, etc., which affect the previously certified and accredited security baseline must be approved by the ODAA (FLTCYBERCOM) prior to installation and use. Software compilers are **prohibited** on the LMD, and removing the hard drive containing LCMS software and replacing it with a hard drive containing non-LCMS software is also **prohibited** at this time.

8. **Access to the LMD/KP**:

Is restricted to personnel performing Key Management functions at the account who have been formally trained on the LMD/KP (EKMS Managers and Alternates only); Clerks will not have access to the LMD/KP. Prospective EKMS Managers and/or Alternates may complete the EKMS JQR discussed in Article 412.f pending completion of formal training.

9. **LCMS IDs / Passwords:**

During initial account/operator registration, ensure that at least **TWO** LMD/KP system administrators are registered within the account. The EKMS Manager and the Primary Alternate must be registered as two of the account's LMD/KP System Administrators. LMD/KP System Administrators are required to perform KP list rollback in the event synchronization is lost between the LMD and the KP. Failure to have at least two registered LMD/KP System Administrators once a loss of synchronization has occurred will prevent the account from being able to perform the KP list rollback and will render inaccessible all data and key stored on the LMD.

NOTES: 1. All Personal Identification Numbers (PINS)/ passwords associated with the LMD/KP must be recorded and sealed in a Safe Combination envelope (SF-700 form), as specified in Article 520. DO NOT record actual PINs in the KP CIK ID Log.

2. Unauthorized adjustment of pre-configured default password settings on the LMD (LCMS SCO password lockout and/or reset) is prohibited per Articles 515.i. and 1005.b.(2).

10. **KP Crypto Ignition Keys (CIKs)**:

Receipt of the transit CIK should occur prior to LMD/KP install. During site initialization, the transit CIK (USKAU B7121) becomes your first user CIK. Destruction procedures must be performed on the transit CIK short title in order to remove it from the Accountable Item (A/I) Summary. Unless specifically directed by the KP, use **only** the port marked "CIK" for all user CIKs. The KP display will indicate when to place a CIK into the port mark "Auxiliary KSD-64." Once you have inserted your user CIK into the KP, **DO NOT REMOVE** until the KP display indicates removal. Removing a CIK prematurely could cause erroneous problems with your KP and require you to shut down the system and log back onto the KP.

> **NOTE: The Transit CIK used when a KP is initialized or reinitialized (as applicable) MUST be recorded as destroyed in LCMS NLT the 5th working day of the month following the month in which it was used. Failure to do so will constitute a non-reportable PDS (late destruction).**

11. **Configuring the KP**:

The KP is usually only configured during site initialization. However, in the event that you must reconfigure the KP, follow procedures in LMD/KP Operator's Manual, Appendix B for "Configure KOK-22A - RS 232 Interface."

12. **Important General Instructions**:

a. All LMD/KP Administrators and Operators assigned KP privileges, must have a unique KP CIK and associated KP PIN. It is strongly recommended that a backup CIK be created for each LMD/KP Administrator. The EKMS Manager must record the following for all LMD/KP Administrators and Operators: name, type (Administrator or Operator), CIK ID, KSD serial number, and date PIN assigned. The CIK ID number is obtained from the KP display window during CIK creation. Whenever the EKMS Manager needs to delete a user's KP CIK, they will be required to provide the CIK ID. The KP CIK ID Log is the only place this information is retained. Once an Administrator or Operator logs on, the PIN is created. It is the EKMS Manager's responsibility to ensure that all PINs are changed every six months.

> **NOTE: All PINs/passwords associated with the LMD/KP must be recorded and sealed in a Safe Combination envelope (SF-700 form), as specified in Articles 515.f and 520.i. DO NOT record actual PINs in the KP CIK ID Log. Two Person Integrity (TPI) must be adhered to when a TS Administrator or Operator CIK is created. This is only applicable for accounts with a HCI of TS.**

b. The KP, monitor, and STE must be arranged/mounted in such a way as to allow the operator to view, without obstruction, the LED windows and screen. This allows the operator to verify the STE display when going secure, and follow commands from the KP display.

c. KP process abort occurs when the KP is involved in any process and requires additional data to complete the process. When additional data is required, you will be prompted to supply it. Failure to supply requested data within one minute results in the process aborting and the KP returning to an idle mode. This can be a catastrophic failure if involved in the re-initialization process.

d. As stated in paragraph 8, once you insert your user CIK into the KP, **DO NOT** remove until the KP display tells you to do so.

e. **NEVER** zeroize an operational KP that is to be replaced with a new KP until the new KP has been initialized and is operational. Only after verifying that the new KP is operational and functioning should you zeroize the old KP in preparation for shipping.

f. When your account is slated for a new KP (for either site initialization or re-initialization) you will receive the KP and Transit CIK in separate boxes. You must check and ensure that the CIK **EDITION** number matches the KP **SERIAL** number. If these two numbers do not match, your KP will not function. In the event of mismatched numbers, contact CMIO immediately and, if applicable, **DO NOT**, zeroize your old KP.

g. Complete an Account Registration form for all EKMS accounts that you will be exchanging data/key within accordance with procedures listed in LMD/KP Operator’s Manual, Chapter 7.

h. Ensure that you properly mark all KP CIKs. The number of CIKs involved in properly maintaining/running your system can become confusing. At a minimum, the label should consist of the CIK name, classification, and date created. See Article 1185 for guidance specific and unique to REINIT 1 and NAVREINIT 2 keys.

i. Once the account's KP and LMD are up and running and the initialization process is complete, the KP is specific to that LMD and will not function with any other LMD. Do not attempt to interchange the KP with another account.

j. Both the FIREFLY Key (USFAU 0000000333) and MSK (USKAU

4294967297) are considered modern key. As such, during the receipt process in LCMS, there are additional key attributes that must be registered for each key. If these attributes are not located on the key tag itself, the following guidance is provided:

(1) FIREFLY KEY
(a) Key type: TYPE 0 SEED FF KEY
(b) Expiration date: YYYYMMDD
(c) SDNS Classification:
T and S (Account HCI = TS)
S (Account HCI = S)

(2) MSK
(a) Key type: TYPE 1 OPER MSK
(b) Expiration date: YYYYMMDD
(c) SDNS Classification:
T and S (Account HCI = TS)
S (Account HCI = S)

NOTE: If expiration date is not listed on the tag for FIREFLY Key and MSK, enter a date of one year greater than the report date listed on the SF-153.

Once used in the KP, both the FF Vector Set and MSK discussed above are to be recorded in LCMS as destroyed using the "Filled In End Equipment" feature in LCMS to remove them from the AIS. For accountability purposes, they are one-time use material and are stored encrypted on the LMD Hard Drive bound to the account data. During a KP Reinitialization the FIREFLY and MSK are retrieved automatically by the KP from the bound data on the LMD and loaded into the new KP. Failure to record them as destroyed (Filled In End Equipment) in LCMS NLT the 5th working day of the month following use is a non-reportable PDS (late destruction).

k. **DO NOT** open the zeroize button housing unless you intend to zeroize the KP. The zeroize button is supposed to be pressed three times within 6-8 seconds to zeroize the KP. In case someone gets curious and does zeroize the KP, remember that your command will have to fund to depot the KP, not to mention the time that your command will be without a KP while awaiting a replacement.

l. If the "Alarm" indicator light illuminates, ensure that you record the error code. This code will assist greatly in determining the cause. After recording the error code, shift the KP to "STANDBY" then back to "ON" to see if alarm clears. If the alarm clears, you may continue using the KP.

m. All dates in the LCMS must be entered YYYYMMDD (i.e., 20000101).

n. **DO NOT** lose or damage your REINIT 1 key. Although the NAVREINIT 2 key may be re-created by performing a changeover, new copies of the REINT 1 key(s) **cannot** be produced. Accordingly, extreme care must be used in the storage and safeguarding of the REINIT 1 key because it is (they are) the only one(s) you have. Failure or loss of the REINIT 1 key will prevent the ability to REINIT a new KP. The loss of that ability will result in the account requiring a new KP, performing a site initialization (vice re-initialization on that KP), and **TOTAL LOSS** of your existing database which would require you to manually enter all of the account data from a COR-generated (hard copy) inventory. See Article 1185 for guidance unique and specific to REINIT 1 and NAVREINIT 2 keys, including the requirement to make backup copies.

o. Once a System Administrator or Operator has successfully logged onto the KP and the KP PIN has been entered, **DO NOT** leave the terminal unattended until the Administrator/Operator has logged off the **KP**. Leaving a terminal unattended after an Administrator or Operator has logged on constitutes a COMSEC Incident in accordance with Chapter 9 (see “Physical Incidents” category, Article 945.e.(5)).

p. When the account receives material accompanied by a hard copy SF-153, and an electronic TRI has not been received, the material must be manually entered into LCMS. To ensure accuracy, enter "Total Lines/Total Quantity" first into LCMS. This way the system will prompt you if, upon completion of entering the short titles, the "Total Lines/Total Quantity" does not match.

q. As stated in paragraph 7, the EKMS Manager and the Primary Alternate must be registered as LMD/KP System Administrators for the account. All other Alternates should be registered as Operators, unless also registered as a System Administrator. In order to perform backups/restorations on the system in accordance with Article 718.d, the LMD/KP System Administrator must have the UNIX "**Root**" account password. The LMD/KP System Administrator should only use the Root password to perform backups/restorations and should not assume any other

UNIX operation system administration responsibilities unless directed by NCMS.

> **NOTE: The UNIX Root account is intended to be the account used by the UNIX Account System Administrator or Information System Administrator (ISA) to perform the functions necessary to maintain the SCO UNIX operating system.**

r. The LMD is hardwired with two serial communications ports. To facilitate the multiple communications requirements for the LMD, one of these two ports was expanded into four ports by installing a 72-pin multi-port connector called a digiboard, located on the back of the LMD. The digiboard cable connects to labeled P1, P2, P3, and P4. These four serial ports are assigned as follows:

PORT	DIGIBOARD CABLE	DEVICE / USE
COM1	P1	DTD/download key from LMD (LMD only accounts)
COM2	P2	Direct COMMS
COM3	P3	KP connects LMD to KP
COM4	P4	ECU Direct/uses TCP/IP (X.400)to connect to EKMS CF

The digiboard cable will be connected to the account's STE terminal via an A/B/C/D switch. The P2 cable should be connected to Position ″A″ to be used for Direct COMMS. The P4 should be connected to Position “B″ to be used for connecting to the EKMS CF Message Server (X.400 connection). The P1 cable should be connected to Position “C″, in order to protect this cable connector when not in use. Position “D″ should remain unused. The STE should be connected to the input/output port of the A/B/C/D switch. The P3 cable should be connected to the RS-232 interface port on the back of the KP, using a 25-to-9 pin adapter. The P3 cable should be connected to the RS-232 interface port on the back of the KP, using a 25-to-9 pin adapter.

> **NOTES: 1. To download key from the LMD to the DTD, the P1 cable is disconnected from Position “C″, and connected to the DTD using an LMD-to-DTD cable connector (LMD only account).**
>
> **2. To receive key from another account into the DTD via the STE, first disconnect the P1 cable from**

Position "C", then connect the DTD to Position "C" using a STE-to-DTD cable connector.

s. Archive. The LMD has a specified amount of space allocated for data storage for each accounting transaction. The only way to remove inactive accounting transactions is to archive the data. The following media may be used for archiving: 35 GB tape; new, not previously used, non-rewritable (CD-R/DVD-R) optical media or 3.5 inch diskettes for archives limited to 1.4MB or less data. Separate media must be used for each archiving session. The operator will be able to specify the starting and ending date of the data to be archived. Once archived, this data can be reviewed and queried, but cannot be altered.

NOTE: Accounting transactions can only be archived if the account has completed processing the transaction and any transactions related to it.

At a minimum, LCMS data must be archived on a semi-annual basis after each fixed cycle inventory, using procedures listed in the LMD/KP Operator's Manual (Chapter 8). More active accounts may need to archive data more frequently. Upon successful completion of the archive, the account must either print out the Archive Media Identification information sheet or transfer the data it contains, by hand, to a sheet that will serve as a label for it. The account must maintain the data identification sheet with the archived data. Archive data must be retained for a period of 4 years from date of creation.

t. Changeover. Is the process of changing the KP Local Key Encryption Key (KEKL) and re-encrypting all of the data on the LMD. The KP encrypts all data stored on the LMD with the KEKL. Based on the cryptoperiod of the KP KEKL, changeover, which must be initiated by the operator following the procedures outlined in Chapter 9 of the LMD/KP Operator's manual. This will update the KEKL and result in the creation of new NAVREINIT 2 keys. More active accounts may need to perform Changeover more frequently. Accounts not performing Changeover will not be able to perform destruction of electronic key when the Electronic key Destruction List (EKDL) becomes full until the Changeover process is performed. Failure to perform changeover as described in Article 238 constitutes a COMSEC Incident and must be reported in accordance with Article 945.

NOTE: Old NAVREINIT 2 keys will be zeroized in the KP).

u. KP Rekey. The cryptoperiod for the Operational EKMS FIREFLY Key is one year. The initial FIREFLY Key (also called FIREFLY vector set) that the account receives will be on a KSD-64A, and loaded into the KP after site initialization. The annual replacement of FIREFLY vector set will be electronically downloaded from the Central Facility (CF) message server. The process of updating the FIREFLY vector set is known as KP Rekey. Initially, after loading FIREFLY SEED Key, and annually thereafter, the account must request the replacement from CF by performing the KP Rekey Request procedures in the LMD/KP Operator's Manual (Chapter 9). Once the account receives the re-key response from the CF, the account must perform the Process KP Rekey Response procedures in the LMD/KP Operator's Manual (Chapter 9) to rekey the KP.

NOTE: 1. The Process KP Rekey Response procedures must be performed prior to, but as close as practicable to, the expiration date of the FIREFLY vector set currently being used by the KP.

2. Prior to initiating KP rekey procedures, the account must reconcile all electronic keying material packages (Bulk Encrypted Transactions (BET)) received from other accounts. Failure to do so will prevent the account from accessing this key once the FIREFLY vector is rekeyed.

v. Importing Key. The procedures for importing key are contained in the LMD/KP Operator's Manual (Chapter 5). The policy governing the importing of physical key (e.g., key tape converted to electronic form) into the LMD/KP is in Articles 740 and 781.

NOTES: 1. If authorized to do so, when importing an entire edition of key, using the DS 102 mode, the operator must have the KP derive the short title for the electronic key, from the short title for the physical key. To accomplish this, the operator must enter the short title from the physical key into the ″Alias S/T″ field and ensure that the "Derive S/T From Alias″ is set to "Yes", in accordance with the procedures in EKMS 704 (series) LMD/KP Operator's Manual (Chapter 5).

2. Tactical units deploying in other than crisis/contingency situations should limit the number of segments loaded into the DTD to those required for the mission. Loading the DTD with key converted from keytape should be limited to those segments

required while the unit is absent from COMSEC support.

3. Whether imported into the KP for transfer to another account or for issue to an end equipment or to a fill device, or when converting hard copy key to electronic form for loading into the DTD, this guidance must be followed: exposed and/or prematurely extracted hard copy key segment(s) should be destroyed immediately after importing/loading, unless there is an operational requirement to retain them. If retained until superseded, they must be stored and accounted for in accordance with Article 775.e.(2).

If an account imports a whole edition of keying material that is AL Code 1, the account must register this key as AL Code 6 in LCMS and must submit a generation report to the COR to bring the electronic version of the short title into accountability.

ANNEX Y

ASSUMING THE DUTIES OF EKMS MANAGER

1. Introduction

a. The purpose of this section is to prepare you to intelligently assume the duties and responsibilities of EKMS Manager. But you must also read and familiarize yourself with the following publications (ask the outgoing EKMS Manager to provide you with copies of these publications and to provide an overview of them as well):

(1) EKMS 1 (series): The rules and regulations governing the operation of an EKMS numbered account are in this publication.

(2) EKMS 704 (series): LMD/KP Operator’s Manual. EKMS 1 series provides you with LMD/KP basics but for an in-depth understanding of the system, refer to this publication.

(3) EKMS 5 (series): The DON Cryptographic Equipment Manual.

b. By following the guidance in these publications carefully and fully, you will have no difficulty in ensuring that you meet the Navy's COMSEC objectives of SECURITY and ACCOUNTABILITY. EKMS 1, EKMS-3 and EKMS-5 series are your most important management tools. Read and refer to these publications often. These pubs, attention to detail, and plain old-fashioned common sense will keep you out of trouble and in good standing with your Commanding Officer and Immediate Superior in Command (ISIC).

c. Because most of you will be taking over an established account, this document is written on that basis and provides a very brief overview of the steps involved in assuming the job of primary EKMS Manager. This document also covers some of the key points, things you should be aware of before you assume the responsibilities for an account. But you must read EKMS-1 (series), EKMS-3(series), and the EKMS 5(series) publications to effectively manage an account.

d. When taking over an account, the NCMS EKMS Manager Turnover Checklist **must be used** as part of the assumption of duties. It will be signed by the outgoing and incoming manager and retained on file in accordance with Annex T to this manual.

2. **Accounting for COMSEC Material**

a. The material you will be working with is COMSEC material. COMSEC material is unique in that each item of material, regardless of its use, is identified by a distinctly different short title, edition, and (in most cases) an accounting number.

b. COMSEC material is accounted for based on its' AL Code. AL 1, 2 and 6 are accountable to the COR. AL4 and AL7 are locally accountable. AL1, AL2, and AL4 are assigned to physical material whereas AL6 and AL7 pertain to electronic key.

3. **Receipting for COMSEC Material**

a. As an EKMS Manager, you will routinely receive physical and electronic shipments of COMSEC material. Regardless of the AL Code assigned to the material you receive, you will be required to report its receipt. You will report receipt using either an electronic or physical SF-153 receipt report.

b. The shipments you receive will originate from one or more of the following:

(1) The NCMS Vault

(2) Vault, Depot and Logistic System (VDLS) (e.g., CMIO Norfolk, USNDA)

(3) Other DON accounts

(4) Non-DON accounts (e.g., Army, Air Force, the National Security Agency (NSA), NSA's Electronic Key Management Central Facility (EKMS CF), contractor accounts).

4. **Inventorying COMSEC Material**

a. As the EKMS Manager, you are responsible for ensuring that you comply with inventory completion and reporting requirements of this manual.

b. All COMSEC material holdings (including publications/manuals and equipment) assigned AL Code 1, 2, 4, 6, and 7 must be inventoried semiannually (twice each calendar year (CY)).

c. Each account is automatically prompted by their respective COR (e.g., DIR TIER1 SAN ANTONIO OR CSLA TIER1) to generate a Semiannual Inventory Report (SAIR) at pre-designated 6-month intervals. The reports are used to both document and report the inventories.

d. The results of both semiannual inventories must be reported to the COR. The results of the semiannual inventories of AL Code 4 and 7 keying material will be retained at the command in accordance with Annex T.

e. Accounts must also conduct inventories upon change of EKMS Manager, Change of Command or Staff CMS Responsibility Officer (as applicable), and prior to disestablishing the account.

5. **Maintaining and Disseminating Material Status**

a. 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 the world of COMSEC, we refer to a material's authorized use date as its effective date. A material's authorized destruction date is referred to as its supersession date. Both the effective and supersession dates of a COMSEC material item are referred to collectively as the material's status.

b. With the exception of COMSEC equipment, almost all COMSEC material is assigned effective and supersession dates. These effective and supersession dates are made available to commands in the Controlling Authority’s COMSEC Effective Status Messages or SIPRNET web page.

c. It is the EKMS Manager’s responsibility to know the status of all COMSEC material charged to the account to ensure that it is used and destroyed within the period promulgated by the Controlling Authority. This responsibility holds true whether the material, is in electronic or hard copy form, remains in the EKMS Manager's vault/safe/LMD or has been issued to the Local Elements (LEs). When an item of COMSEC material has reached its assigned effective date, it is authorized for use. When an item of COMSEC material has reached it assigned supersession date, it is authorized for destruction.

AMD-9

d. The EKMS Manager must ~~advise~~ provide LE personnel ~~of the~~ with status information of materials issued to them. The

EKMS Manager must be especially vigilant when it comes to maintaining material status because status changes occur with regular frequency. Status changes occur for routine reasons as well as for emergency reasons (e.g., the material is strongly suspected of having been compromised). Status changes are disseminated in general messages (e.g., ALCOMs), via messages originated by Controlling Authorities, and on the Controlling Authorities' SIPRNET web pages. Accordingly, before issuing materials for use or before destroying materials, the EKMS Manager must always check the latest COMSEC Effective Status Messages from the Controlling Authority.

6. **Destroying COMSEC Material**

a. As an EKMS Manager, you will be responsible for overseeing the proper destruction of COMSEC material issued to LEs and for destroying unissued COMSEC material (material that has not been issued for use but which remains in the account vault/security container).

b. You will oversee the proper destruction of issued COMSEC materials by ensuring your LEs receive accurate status information and submit required destruction documentation to you in a timely manner. Each month, you will collect the destruction records completed by your LEs and use them to complete the command's consolidated SF-153 destruction record of material destroyed for that month. The Local COMSEC Management System (LCMS) provides the capability to automatically prepare Destruction Reports for reportable material and locally accountable material.

7. **SF-153 Signature Requirements**

a. As the EKMS Manager, you will generate and use SF-153s to document transactions involving COMSEC material.

b. Hard copy SF-153s used to document any one of the following transactions will always require the signatures of three people: yours, an EKMS witness (who may be the alternate manager), and the commanding officer (or executive officer when the CO is absent).

NOTE: Duties of the SCMSRO cannot be further delegated and must revert to the appointing official in the absence of the assigned SCMSRO.

(1) SF-153 Fixed-Cycle Inventory/SAIR

(2) Change of Command or Staff CMS Responsibility Officer (SCMSRO) Inventory (as applicable)

(3) Change of EKMS Manager Inventory/CCIR

(4) Relief from Accountability Report

(5) Possession Report

(6) Consolidated Destruction Report

(7) Generation Reports

NOTE: When an inventory of electronic key is performed entirely by an EKMS component, such as the LMD/KP, a witness is not required. A witness is required for an inventory of keys in a DTD/SKL if the audit information is not examined.

c. SF-153s (COR-reportable and locally prepared) used to document the receipt of all COMSEC material (includes crypto equipment and CCIs) minimally require two signatures: yours (or an alternate acting in your behalf) and an EKMS witness. See Annex U for signature requirements specific to two-person control (TPC) material. The outgoing Manager should have advised you of any TPC materials that may be managed in the account and about TPC control procedures.

8. Page Checking COMSEC Material

a. The page checking of COMSEC material is a very important part of assuming the duties of EKMS Manager. Page checking ensures the completeness of COMSEC material.

b. The term "page checking" is another word for sight-verifying the segments of unsealed (i.e., not protectively packaged) keying material and the pages of unsealed classified publications. Page checking is also used to refer to the sight verifying of various components of COMSEC equipment and related devices.

c. The importance of proper page checking cannot be overemphasized. For example, if a classified page from a manual is missing, you have a reportable COMSEC incident on your hands. Something you want to avoid! To minimize the occurrence of such incidents, ensure all unsealed keying material and unsealed classified publications are page checked during the change of EKMS Manager inventory and at prescribed intervals thereafter. Page checking policies (procedures, timeframes, items to be page checked and the reporting of discrepancies are outlined in, Article 757 and Annex V.

9. The Mechanics of Assuming Duties as A Manager: The Inventory

a. All COMSEC material holdings must be inventoried on the occasion of a change of EKMS Manager.

b. A CCIR Report is used to officially document the change of EKMS Manager. The CCIR will be created by the account and sent to the COR for reconciliation.

c. The account must notify the COR prior to sending the CCIR.

d. In conducting the change of EKMS Manager inventory, you must either personally sight each copy of each item of material listed on the inventory, perform the inventory using EKMS components, or you must obtain written certification from the individuals holding the material (e.g., your LEs) that they do, in fact, have the material in their possession.

e. You must also page check all the unsealed COMSEC materials as discussed above, or you may detail someone else to do it for you. If you don't personally conduct these required page checks, then others who assist you must certify in writing that they have indeed done them and must report discrepancies to you.

f. Accepting written certification from LEs instead of personally sighting the material yourself should be resorted to **only when it is not feasible for you to visit a remote LE location, or if the material is held in spaces to which you normally would not have access because of special security requirements.**

g. The written certification you accept under such circumstances should be a naval message, letter, or signed memo.

h. Once you sign the inventory report, you are certifying the following to the Central Office of Record for COMSEC material:

(1) That you have either seen each item of material

listed on the inventory or that you have written certification from the LEs of the material that the items are in their possession; and,

(2) That you are taking responsibility for all the material listed on the inventory, as of the date of the inventory, until a new EKMS Manager assumes the duties and responsibilities.

10. **Verify that Keying Material is Being Properly Maintained**

a. Another important aspect of assuming the duties of primary EKMS Manager of an account is verifying that keying material in use is being properly maintained. We strongly recommend that you review the local records of destruction for material currently being destroyed by LEs of the account to ensure the following:

(1) That two signatures appear for every segment of keying material that has been destroyed. (Ditto marks, connecting lines, etc., **are prohibited**.)

(2) That a date of destruction appears for every segment destroyed and the dates comply with the destruction timeframes in EKMS 1B. Again, no ditto marks, connecting lines, etc., are allowed.

(3) That the command is using appropriate local destruction records (i.e., locally prepared records contain all required fields of information). (See Chapter 7 of this manual; Figures 7-1, 7-2, and 7-3).

b. Improperly completed forms can constitute either a Practice Dangerous to Security (PDS) or a COMSEC Material Incident depending on the type and amount of information that has been omitted.

c. **Management of Modern Key**: This is a very important aspect of account management. Please review Annex AE and ensure User Representative privileges are established or modified, as applicable when assuming the duties of the EKMS Manager. Failure to do so may impact operational readiness as Modern Key is not automatically distributed based on a profile; it must be ordered. Also verify the accounts holdings are sufficient and that the modern key reflected as “on-hand” in LCMS is not expired.

AMD-9

11. **Review the Command's Last ~~CMS Inspection~~ COR Audit Report**

a. In addition to completing the required Change of EKMS Manager inventory, new managers should; (a) review the results of the last ~~ISIC inspection~~ COR Audit, (b) review the results and/or recommendations of the last ~~CMS A&A~~ assist visit, if applicable, and (c) review the account's completed spot checks and any messages or memorandums submitted related to both Incidents and Practices Dangerous to Security (PDSs).

AMD-9

b. For discrepancies from the previous ~~inspection~~ audit or recommendations from the last ~~CMS A&A~~ training visit, inquire and verify that they have been resolved or what the status of these items currently is.

c. Remember, if you find anything wrong during the change of EKMS Manager process, you have the right and responsibility to report the errors, COMSEC material incidents, or other problems to the Commanding Officer of the account. You should also make these errors or irregularities a matter of record at the time you accept the responsibility for the account, especially if you can't get them fully squared away before taking the job.

12. **READ, READ, READ! Knowledge is your Best Defense!**

a. As stated earlier in this document, the foregoing is a very brief overview of things to do or to be aware of before assuming the duties as EKMS Manager of an existing account. You must read and familiarize yourself with; EKMS-1, EKMS-3, EKMS-5, and various Operational Security Doctrine promulgated by NSA (for COMSEC equipment charged to/used by the accounts Local Elements). Do not neglect to familiarize yourself with the COMSEC material incidents and Practices Dangerous to Security (PDS) sections in the EKMS-1 (series). Attention to detail and understanding the impact (potentially globally) that Incidents and PDSs have on matters of National Security cannot be overemphasized.

AMD-9

b. If a situation is discovered and the appropriate course of action or significance of the matter is not known consult the applicable chapter in the EKMS-1 publication and if the matter remains unclear, contact your servicing ~~A&A training~~ COR Audit team or NCMS N7 or N5, in this order for assistance. Contact information can be found in Annex S of this publication.

EKMS MANAGER TURNOVER CHECKLIST

Item	Conducted by	Witnessed by	Remarks
Pending Receipts	Outgoing Manager	NA	(1) Request an up-to-date Pending Receipts Report from NCMS. (a) For any physical material reflected with a TN date 30 days or longer, **the outgoing manager will report non-receipt to the command which initiated the transfer.** (b) If any electronic key is reflected, the outgoing manager will connect to the X.400 message server, download the material (BETs) in the mailbox and submit the receipts or report of corrupt BET, as applicable within 96 hours in accordance with EKMS-1(series) Article 742. (c) If any BETs cannot be processed and they contained modern key, it **MUST BE REORDERED**. *Tier-1 cannot resupply modern key.*
Change of Manager Inventory	Outgoing Manager	Incoming Manager	Requires 100% sight inventory of all COMSEC material (less embedded COMSEC installed in equipment) including keying material, book-packaged material, equipment, CIKS, etc… * **Ensure KAMs, KAOs, Q-kits and book-packaged material is page checked and such is recorded in the Record of Page check page**. Also ensure all Inventory Reconciliation Status Transaction (IRST) discrepancies are corrected or the required action has been taken **PRIOR TO** assuming the account.
Verify Reserve on Board (ROB) levels	Outgoing Manager	Incoming Manager	Ensure levels are adequate for operational requirements. See the matrix in EKMS-1B Article 620 and report shortages to NCMS and CMIO. Example: If the edition supersedes annually the unit should have a minimum of the current +1; semi-annually the current +2, quarterly the current +2. **Do not have only the currently effective edition of key and no ROB as an emergency supersession will result in a critical circuit outage or possible COMSEC incident.**
Pending Outgoing Transactions	Outgoing Manager	Incoming Manager	Ensure receipts for any material transferred are processed. To verify if any outstanding transactions exist, go to: **Accounting – Reconcile – Hard Copy Receipt or Accounting- Reconcile – Electronic Receipt, as applicable**. Contact the recipient to verify the material was received and request the receipt be returned for processing.
Verify Modern Key holdings	Outgoing Manager	Incoming Manager	**Ensure a minimum of 05 copies of modern key required for each network/enclave are ordered prior to turning over the account**. Go over each supported network/enclave with the incoming manager. If any are closed partitions, ensure Command Authority information is part of the turnover.
Modern Key Expiration Data	Outgoing Manager	Incoming Manager	(1) Review expiration date information for all modern key held **with emphasis on any expiring within 60 days or which is AOR specific, if deploying. For any not ordered above, ensure key orders are submitted.** (2) Verify the use of the NCMS modern key tracking tool. If not in use, download it, populate the data and make use of it. It can be found via SIPR https://uar.cas.navy.mil/secret/navy/39/portal.nsf **- Modern Key Forms – Modern Key Tracker** **** Remember, modern key doesn't just end up in the units X.400 mailbox; it must be ordered****
Update Common Account Data (CAD)	Outgoing Manager	Incoming Manager	Ensure the accounts CAD data is updated to reflect the new EKMS Manager. See EKMS-704 Chapter 7 (Request EKMS Account Modification)

Update User Registration Data (CF 1206)	Outgoing Manager	Incoming Manager	Update the Central Facility User Representative (UR) Ordering Data. Forms and instructions can be found at: https://www.iad.gov/KeySupport/index.cfm
DTD/SKL Audit Review Log	Outgoing Manager	Incoming Manager	Verify the log exists for the current year and prior (02) years. If the log does not exist, submit a COMSEC incident report in accordance with EKMS-1B Article 945.E.4.
Combinations/Pins/ Passwords	NA	Incoming Manager	(1) Ensure combinations held by the prior manager(s) are changed and SF-700s are updated and properly stored. (2) Ensure any passwords, including the root password for the LMD or KP pins are changed and recorded on a new SF-700.
Update the USTRANSCOM Form-10	Outgoing Manager	Incoming Manager	Ensure accurate reflection of the new Manager and other account personnel and submit it to the servicing DCS station. EKMS-1(series) Art 405.h;.Annex I. The form can be found via SIPR https://uar.cas.navy.mil/secret/navy/39/portal.nsf - EKMS Documents – Common Forms for Managers and LE
Update the CMS Form-1	Outgoing Manager	Incoming Manager	(East Coast units only) . EKMS-1(series) Art 405.H; Art 640; Annex H . The form can be copied and edited from the sample in Annex H.
Access List Updates	NA	Incoming Manager	Ensure the vault access list is updated. EKMS-1(series) Art 505.D.
Letter of Appointment	Outgoing Manager	Incoming Manager	Ensure the Incoming Manager is properly cleared, appointed in writing and executes a SD Form 572. EKMS-1(series) Art. 412, 418, 505, Annex K
KP Changeover	NA	Incoming Manager	Conduct a KP Changeover, label the new NAVREINIT 2s properly, conduct a LMD backup and zeroize the old NAVREINIT 2s (EKMS-704 9-65). Ensure future KP Changeovers occur every 92 days at a minimum. (EKMS-1B Art 238.B.2; Art 945.C.8)
KP Rekey	NA	Incoming Manager	(1) Verify there are **no** BETs on the desktop. If so, unwrap them and reconcile for the material. (EKMS-704 Paragraph 10-24, 10-7, 4-48). (2) If any BETs cannot be unwrapped/processed follow the BAD BET procedures in EKMS-1(series) Art. 742.D (3) Conduct the KP Rekey (EKMS-704 9-17), process the Rekey Response and post the new credentials by connecting to the Directory Service and "UPLOAD OWN" CAD.
Status Information	NA	Incoming Manager	Do not carry out destruction or issue material without first verifying the accuracy of status information applied to the material or reflected in LCMS.
General Message Review	Outgoing Manager	Incoming Manager	Verify all COMSEC-related ALCOMs, ALCOMPAC P (PACFLT units) and ALCOMLANT ALFA (LANTFLT units) is held. Start with the most recent recap which is ALCOM, ALCOMPAC P or ALCOMLANT ALFA 001/XX (XX = CY)
Command COMSEC Policy	NA	Incoming Manager	Review the Command, ISIC and TYCOM COMSEC policies.
Transit CIK, FF Vector Set, and MSK	Outgoing Manager	Incoming Manager	Verify there are no previously loaded Transit CIKS, FF Vector Sets or MSKs on the Accountable Item Summary (AIS) : EKMS-1(series) Article 238; 1005.A (Note: You will always get a new Transit CIK when the KP is replaced. The Transit CIK (USKAU B7121) when loaded becomes the 1st sysadmin CIK and must be recorded as destroyed. The MSK when loaded created the REINIT1 and NAVREINIT 2 KSD-64As and also must be recorded as destroyed. The FF Vector Set (USFAU 0000000333), when loaded is used to enable generation and exchanging of credentials to exchange or receive electronic keying material. It is a SEED key and must be recorded as “Filled in End Equipment” not “destroyed” when loaded. It is kept up-to-date through the required annual KP Rekey.
KP Recertification	Outgoing Manager	Incoming Manager	Verify the certification date on the accounts KP. If it expires in six months or less or the command will be at-sea when it expires coordinate early

			replacement with CMIO and NCMS. EKMS-5(series) Article 202
Backups & Archives	Outgoing Manager	Incoming Manager	Verify backup media and archives are on file, labeled and safeguarded at the secret level. A LCMS backup is highly recommended during assumption of duties to ensure an up-to-date tape is available should the LMD fail.
Review Letters of Agreement	Outgoing Manager	Incoming Manager	If support is provided to external LEs a LOA is required. They must also be updated every 3 years or upon Change of Command, whichever occurs sooner. EKMS-1(series) Art. 445.
Review the most recent CMS AA visit report	Outgoing Manager	Incoming Manager	Identify discrepancies noted, if any and what corrective action was taken.
Review the commands last ISIC inspection	Outgoing Manager	Incoming Manager	Identify discrepancies noted, if any and ensure the discrepancies have been corrected.
Conduct an account Self-Assessment	Outgoing Manager	Incoming Manager	At a minimum Annex A to EKMS-3C will be used. If time permits, a minimum of (3) LEs should also be assessed using Annex C to EKMS-3 (series).
Training	Outgoing Manager	Incoming Manager	Review the commands long and short-range training schedule and ensure COMSEC training in part of the schedule. EKMS-1(series) Art. 455.F
Spot Checks	Outgoing Manager	Incoming Manager	Review spot checks completed by the CO and the EKMS Manager(s). 16 total are required per year (Art 450/455/1005.A.17). (4) by the CO; (2) of which can be delegated and (1) per month by the EKMS Manager or Alternate(s).
KAMs/KAOs/ Q-kits	Outgoing Manager	Incoming Manager	If excess copies are held, the account has KAMs/KAOs or Q-kits for equipment no longer held, or the account have broken CCI in the account, request disposition instructions for these. EKMS-1(series) Art. 655 and EKMS-5(series) Art 402-403. San Diego ships, mobile units, etc… can use the COMSEC Equipment Exchange Program (CEEP) to have broken CCI replaced through the CRF in San Diego, when assets are available to replace the failed units. See EKMS-5(series) Art. 403 **(Note: Don't go to sea with broken CCI)**
If incidents and/or PDSs are discovered, ensure they are documented and reported, as required. They are not like sores and heal over time with a little Bacitracin. They are likely to be discovered during a visit and/or inspection however, if self-identified and documented/reported, as applicable the unit cannot be cited again. Don't have the mindset, it happened before my time. Be engaged and provide training and oversight to the other alternates and LE personnel alike.			

I/we certify herein that the actions and areas identified herein have been completed or reviewed and found current and up-to-date.

Outgoing EKMS Manager		Incoming EKMS Manager	
Printed Name	Grade	Printed Name	Grade
Signature	Service	Signature	Service

FIGURE Y-1

ANNEX Z

AN/CYZ 10 OR DATA TRANSFER DEVICE (DTD)

PART I

1. Purpose

To prescribe the minimum policies and procedures for the handling, safeguarding, and accounting of DTDs and related materials. These procedures are intended to provide maximum flexibility, yet ensure that proper security and accounting controls are in effect to preclude the loss of this material and the compromise of the information it protects.

The DTD is an integral component of the EKMS. It is used to securely distribute key generated by the LMD/KP to consumers. The consumers are either an end cryptographic unit (ECU) or another DTD. The DTD is also able to replace current common fill devices (FDs).

The DTD has a host side and a COMSEC 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 COMSEC side performs the cryptographic functions.

This Annex is divided into two parts: Part I contains the safeguarding and handling policy for the DTD and provides limited guidance on DTD repair. Part II provides definitions of unique terms used in Part I (unique terms are italicized where they first appear in Part I).

Procedures for operation of the DTD are contained in the DTD User's Manual (ON477340) and DON AN/CYZ 10(V)3 DTD Operator's Manuel (PMW161-DTD-OM-1), dated December 1996.

2. **References**

* Data Transfer Device (DTD) User's Manual (ON477340)

* DON AN/CYZ 10(V)3 DTD Operators Manual (PMW161-DTD-OM-1) (Dec 1996)

* Field Generation & Over-the-Air Distribution of COMSEC Key in Support of Tactical Operations and

Exercises (NAG 16 Series)

3. DTD Description

The DTD is a small, lightweight, electronically programmable fill device in a ruggedized case. The DTD has a keyboard for input of commands and an alphanumeric screen to display the status of the unit and operator instructions.

The AN/CYZ 10 is the full keyboard version and the AN/CYZ 10A is the limited keyboard version of the DTD.

For compatibility with existing equipment, the DTD has a 6-pin Input/Output connector and will operate according to DS-101, DS-102, RS-232, and MIL-STD-188-114 interface specifications.

A fill device application program is provided with the DTD to perform functions comparable to those currently performed by the KYK 13, KYX 15A, and KOI 18. This software also allows the DTD to handle keys with lengths other than 128 bits.

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.**

4. DTD Capabilities

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 less than 1000.

The DTD can securely store key of all classifications and categories on the COMSEC side. On the host side, data classified up to Secret may be processed, stored, or transmitted.

The functionality of the DTD is dependent on the application software that resides in it.

5. **Crypto Ignition Key (CIK) Description**

The DTD uses a CIK to control access to the cryptographic capabilities of the device. The CIK is black in color, circular, and approximately 3/4” in diameter and 1/2” long. At the top of the CIK are two protrusions to secure the CIK in the DTD. There is also a metal halyard ring that is used to attach the identification label. In general, when a CIK is inserted in the DTD and the DTD is powered on, the cryptographic capabilities of the DTD are unlocked to allow the input/output and handling of key and other information.

There are two types of CIKs: User and Supervisory. *User CIKs* allow the DTD operator to perform all the basic handling and distribution functions of the DTD. The *Supervisory CIK* has all the privileges of the User CIK and additionally allows the *Supervisory User* access to all the DTD's functions, including the Utilities and Setup default applications.

In addition to controlling access based on supervisory versus user privileges, the DTD's CIKs can also be used to control access to key stored in the DTD's key storage database. The DTD's key storage database can be divided into compartments with access to the key in the different compartments granted only to users with specific CIKs.

6. **DTD Keying**

a. **Types of Key**. The DTD handles two types of key: DTD key and User key. DTD key is needed for the DTD's own internal use. The User key is key which is stored and transferred by the DTD for use by other cryptographic devices, equipment, and systems.

b. **DTD Key (or Internal Use Key):**

(1) *Storage Key Encryption Key* (SKEK) also referred to as Local Key Encryption Key (LKEK)is used to store keys in the DTD's storage database in encrypted form to prevent exposure to the keys when the associated CIK is removed. SKEK is generated by the DTD when the DTD is initialized with the CIK. It is split and inaccessible when the CIK is removed, but recombined and accessible when the CIK is again inserted. When the DTD's key storage database is compartmented, there is a unique SKEK per compartment.

(a) The LMD/KP can generate the SKEK. This process is completed by the LMD/KP generating the SKEK and distributing it in an ECU (i.e. DTD). Once the fill is complete the LMD/KP will record the key as being destroyed and remove it from the account's AIS (**EXAMPLE:** 100 SKEK segments were generated and the account filled 5 DTDs (1 segment ea.) with the key. The LMD/KP will show 95 segments remaining vice 100 on the AIS. Additionally 5 segments will be placed on the end of month destruction report, and annotated "Filled in Equipment"). The SKEK within the DTD will remain effective until zeroized or superseded.

NOTE: Before reinitializing a CIK to create its new SKEK, ensure that the DTD is not storing keys protected by the CIK's current SKEK. Once the CIK is reinitialized, such keys cannot be recovered. Documentation must exist to verify reinitialization of DTDs occur annually. This can be accomplished by uploading and printing the audit trail after initializing/reinitializing a DTD or through adding a column and recording such in the Audit Trail review log. A sample DTD/SKL Audit Trail/Reinitialization log can be found on the NCMS CAS portal.

(2) *Transfer Key Encryption Key* (TrKEK) may be used in the DTD to output previously encrypted user key (key loaded into the DTD as encrypted key) in unencrypted form. The TrKEK will usually be filled into the DTD via the KP (KOK-22A), but may be filled into the DTD from another DTD.

NOTES: 1. When TrKEK is loaded into a DTD storing keys encrypted with that TrKEK, the keys are considered unencrypted when the CIK is inserted (see paragraph 8 for effect on overall DTD classification). To minimize DTD handling and safeguarding requirements, do not load TrKEK into the DTD until the keys need to be decrypted for use.

2. To the extent possible, TrKEK should be pre-positioned or sent to the destination in a separate path from the DTD. See paragraph 24 for OTAT of new or replacement DTD TrKEK between communicating DTDs secured by a STE.

c. **Cryptoperiods.**

(1) DTD-generated SKEK has a one-year cryptoperiod.

(2) Transfer Key Encryption Key (TrKEK)

a. Three-month cryptoperiods should be used for most data transfer device (DTD) TrKEKs. CONAUTHs may assign a one-year cryptoperiod to TrKEK used for point-to-point circuits and small cryptonets.

b. When operationally required, DTD TrKEKs may be stored in DTDs for up to twelve months before their effective dates.

d. **Classification and AL Code.**

(1) SKEK is classified according to the highest classification of key it secures in the DTD. DTD-generated SKEKs do not have an AL Code since they are never handled outside the DTD. SKEK generated by the LMD/KP will be assigned AL Code 7.

(2) TrKEK is classified according to the highest classification of material it secures and is designated CRYPTO. TRKEK generated by the LMD/KP will be assigned AL Code 7.

7. **DTD & CIK Accounting Requirements & CIK Serial Number Assignment**

a. The **DTD** is accountable to the COR as AL Code 1 material.

b. The **CIK** is locally accountable to the EKMS Manager by assigned serial number. The policy for CIK serial number assignment follows.

c. 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 CIKs.

NOTE: During account inventories, valid CIKS (supervisor and/user) will be reflected on a locally generated SF-153 and reflected using either DTD Supervisor or DTD User CIK, as applicable, QTY 1, the beginning/ending serial number will be the serial number of the CIK The ALC code will remain blank or reflect NA.

8. **DTD Classification & Handling**

a. The DTD is unclassified CCI until:

(1) The DTD contains classified data on the *host side*

(whether or not CIK is inserted),[7]

or

(2) An associated CIK is inserted that can output classified (unencrypted) key from the DTD.

b. When only (1) is true, DTD assumes classification of data.

c. When only (2) is true, DTD assumes classification of key.

d. When both (1) and (2) are true, the DTD assumes the higher classification.

e. When the DTD contains key previously encrypted in a TrKEK (loaded into the DTD as encrypted key), and users are denied access to that TrKEK, DTD is UNCLAS CCI (whether or not CIK is inserted) **or** DTD assumes classification of host side data, whichever is higher.

f. When keying material is loaded inside the DTD, a classification tag should be attached to the lanyard indicating the highest classification level of key stored within. When the CIK is inserted handling requirements will be maintained in accordance with the classification level of its associated DTD. A sample tag label would be 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.

9. **CIK Classification & Handling**

a. The CIK by itself is unclassified. In other than a watch environment, the CIK shall be stored separately from the DTD. With the CIK inserted, the key stored within is accessible and the DTD shall be classified, safeguarded and stored based on the highest level of key stored therein.

[7] The CIK does not control access to the data on the host side of the DTD. That data can be viewed without the CIK being inserted.

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

c. A CIK that can output only encrypted key from the DTD is unclassified, providing the TrKEK used to pre-encrypt the key is inaccessible to users.

d. A tag must be attached to the CIK (e.g., via chain) to identify the highest classification level and serial number of the CIK.

e. If a CIK fails to work, the update count will be verified. If the update count in the DTD is higher than on the CIK, it means an unauthorized copy of the CIK has been used in the DTD and the key should be considered compromised. See paragraph 26 (Reportable COMSEC Incidents).

10. **TPI Requirements**

a. CIKs that allow output of unencrypted TOP SECRET key designated CRYPTO require TPI handling and storage.

b. When authorized users will not be present, a TOP SECRET CIK must be removed from the DTD and returned to TPI storage. Otherwise, both the CIK and DTD must be continually safeguarded according to TPI rules.

c. 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 individual(s) 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.

d. **Exceptions** to TPI Requirements:

(1) Mobile Users or Navy Expeditionary Combatant Commands (NECC) (e.g., 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.

(2) Aircraft: TPI is not required during the actual loading process in the aircraft, but TPI is required up to the

flight line boundary (assuming DTD and TOP SECRET CIK are being hand-carried simultaneously).

NOTES: 1. TOP SECRET CIK(s) placed in an Air Crew comm box locked with TPI-approved combination locks fulfills TPI requirements. Consequently, one aircrew member may transport the locked comm box up to the flight line boundary.

2. TOP SECRET CIK(s) may be stored onboard the aircraft in a single-lock container while the aircraft is in a flight status.

(3) Flag (e.g., COMFLT) communicators operationally deployed away from their primary headquarters are exempt from TPI requirements.

11. DTD/CIK Clearance & Access Requirements

a. A clearance is not required to externally view a CIK (Supervisory or User, classified or unclassified) or a DTD that contains no key or data. Neither is a clearance required to externally view an *unkeyed DTD* containing classified key designated CRYPTO or data.

b. Unrestricted access to a DTD or to a CIK associated with a DTD containing the keying material requires a clearance equal to the level of handling required in paragraphs 8 and 9, respectively.

c. Unrestricted access to a DTD keyed with a classified CIK or to a classified CIK also requires written access authorization per Chapter 5.

d. Unrestricted access to Supervisory CIKs must be limited to those who are authorized to perform all of the privileges allowed by the Supervisory CIK.

12. Storage of Key in the DTD

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 at any time. The only exception to the “one canister” rule per DTD is that the follow-on canister of keying material can be loaded into the DTD at any given time during the final month prior to the current edition being superseded.

b. There is no limitation on the length of time that user key may be stored in the DTD. However, superseded key must be destroyed in accordance with paragraph 15 guidance.

c. Key must **not** be stored on the DTD host side. Report any known violations of this rule in accordance with paragraph 26.

13. **Issue and Receipt of Key in DTD**

a. Segments and/or entire editions of key of all classification levels may be issued in a DTD for further issue or use.

> **NOTE: When electronic key converted from keytape is loaded into the DTD, the keytape segments can be destroyed unless there is an operational requirement to retain them until superseded. If retained until superseded, they must be stored and accounted for in accordance with Article 775.e.**

b. When issuing key to a DTD from the KP it is recommended that prior to the issue that the AN/CYZ 10 equipment registration time out be changed from 600 to 900 milliseconds to alleviate KP time outs. This is especially important when transferring electronic key because if a time out occurs during this process the key is not transferred to the DTD and it will also be removed from the accounts AIS. To change the AN/CYZ 10 time within LCMS perform the following:

- Click on "Registration"
- Click on "Equipment Type"
- Click on CYZ10 or ANCYZ10 (may vary depending on how the equipment type was originally entered into the account)
- Click on "Modify"
- Look for Equipment Response Time Out and change it from 600 to 900
- Click on "Register Type"

c. Operational requirements and logistical constraints will dictate how much key may be issued to users in a DTD. However, the amount issued must be kept to the minimum required to support operations so as to minimize the effects of a compromise. General guidelines for issue follow:

(1) Tactical units deploying in other than crisis/contingency situations should limit the number of segments

loaded into the DTD to those required for the mission. Loading the DTD with key converted from keytape should be limited to those segments required while the unit is absent from COMSEC support. The exposed and/or prematurely extracted hard copy key segment(s) should be destroyed immediately after loading into the DTD, unless there is an operational requirement to retain them. If retained until superseded, they must be stored and accounted for in accordance with Article 775.e.

(2) Units deploying under real world crisis/contingency scenarios may download the current edition plus the minimum amount of keying material necessary for the crisis scenario, up to a maximum of 120 days keying material, into a DTD. Common FDs (i.e., KYK 13 and KYK 15) may not be used for this purpose. Requests for extensions in excess of 120 days must be forwarded to NCMS WASHINGTON DC//N5// (information copy to DIRNSA FT GEORGE G MEADE MD//I01P22//).

d. Recipients of key issued in a DTD from an LMD/KP will acknowledge receipt of the key by signing local custody documents. Minimum accounting information for the key will include:

(1) short title(s) or designator(s)

(2) date of generation and/or loading

(3) date of issue or transfer

(4) identity of issuers and recipient(s),

NOTE: For key issued via DTD-DTD or SKL-DTD or loaded from paper tape, such will be documented as outlined in Article 769.h.1.

14. **Local Inventory Requirements**

a. For Other Than Watch Station Environment:

(1) Supervisory and User CIKs must be inventoried whenever the account conducts semi-annual (fixed-cycle), Change of Command, Change of EKMS Manager or combined inventories and will be reflected by serial number on a locally generated SF-153 **(see the note to paragraph 7.c above for guidance in how to properly reflect CIKS on locally generated SF-153s).** The EKMS Manager or Supervisory User may direct more frequent inventories. The window display of each DTD will also be verified to ensure that all CIKs (Supervisory and User) associated with each key in the DTD are

visually verified.

Note: There are no inventory requirements for blank CIKS not in use/associated with a device.

(2) The EKMS Manager (or Alternate) must inventory Supervisory CIKs. The EKMS Manager may delegate the responsibility for inventorying User CIKs to the Supervisory User.

(3) The results of local inventories are reportable to the EKMS Manager.

(4) Failure to inventory in-use/associated DTD CIKS during inventories will be documented in accordance with Article 1005.a.

b. For Watch Station Environment:

(1) The serial numbers of Supervisory CIKs, User CIKs, and DTDs will be visually verified whenever watch personnel change. The watch-to-watch inventory will serve as the record of inventory. See Article 1181 for inventory requirements for electronic key.

(2) The oncoming watch supervisor and an EKMS witness will inventory all Supervisory CIKs. The oncoming watch supervisor will designate appropriately cleared and authorized personnel to inventory User CIKs and DTDs.

(3) Inventory discrepancies will be reported immediately to the Supervisory User and the EKMS Manager (or Alternate).

(4) For account inventories, i.e. semi-annual, change of EKMS Manager, change of command, etc… both Supervisor and User CIKS will be inventoried as reflected in the note to Paragraph 7.c of this annex and Paragraph 14.a.1 above.

15. **Destruction of Key in DTD**

a. **Emergency Supersession Guidance for EKMS Managers and DTD Users.** Destroy/delete emergency superseded key as soon as possible and always within 12 hours of receipt of emergency supersession notification.[8]

[8] The only authorized exceptions to this 12-hour destruction standard are in paragraphs 15b(1)(b) and 15b(1)(c).

b. **Routine Destruction Guidance for DTD Users.**

(1) Regularly superseded key: Destroy/delete superseded key as soon as possible after the end of the cryptoperiod and always within 12 hours after the end of the cryptoperiod. The only authorized exceptions to this 12-hour destruction standard follow:

(a) Users need not remove classified CIKs from secure storage for the sole purpose of performing routine destruction of superseded segments. Users may postpone destruction of superseded segments until the entire edition is superseded or until the next use of the DTD, 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.

(b) 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.

(c) Superseded keying material on board an aircraft is exempt from the 12-hour destruction standard. However, superseded keying material must be destroyed as soon as practicable upon completion of airborne operations.

(2) Irregularly superseded key whose supersession is promulgated by message: Destroy as soon as possible after receipt of supersession message and always within 12 hours of receipt.[9]

(3) Destroy on-the-air test key at the end of the testing period as determined by the test director.

c. **Routine Destruction Guidance for EKMS Managers.**

(1) Regularly superseded key: EKMS Managers storing key in DTDs are authorized to postpone routine destruction of superseded segments until the entire edition is superseded, or until end of month destruction. If held until end of month destruction, destroy material no later than five working days after the end of the month in which the edition is superseded.[10]

[9] The only authorized exceptions to this 12-hour destruction standard are in paragraphs 15b(1)(b) and 15b(1)(c).

[10] The only authorized exception to this destruction standard is in paragraph

(2) Irregularly superseded key whose supersession is promulgated by message: EKMS Managers may retain superseded key until end of month destruction. If held until end of month destruction, destroy material no later than five working days after the month in which supersession occurred.[11]

d. **Documentation Requirements.** There is no requirement to document destruction of key in a DTD. DTD Audit trail reviews will serve to verify deletion/destruction of key. See paragraph 17 for audit trail review requirements.

The loss of Traditional or Modern Key as a result of a device failure or database corruption must be reported to the supporting Account Manager as discussed in paragraph 8 to Annex AE.

16. **Transportation Guidance**

a. Shipping the **DTD**

(1) **The DTD must always be shipped separately from its associated CIK(s) once the CIK(s) are initialized, whether or not the DTD contains keying material or host side data.**

(2) When the DTD contains no keying material and no classified host side data, transport using any of the means approved for UNCLAS CCI in Article 535.

(3) When the DTD contains only keying material (or keying material and unclassified host side data), and providing the corresponding CIK(s) are shipped separately, transport using any of the means approved for UNCLAS CCI in Article 535.

(4) When the DTD contains only classified host side data (or keying material and classified host side data), and providing the corresponding CIK(s) are shipped separately, transport using any of the means approved in Article 530.c. for the classification level of host side data.

b. Shipping the **CIK**

The CIK must be shipped separately from its associated DTD, using any of the means approved in Article 530 for keying material of its classification. (See paragraph 9 of this annex

15b(1)(b).

[11] The only authorized exception to this destruction standard is in paragraph 15b(1)(b).

for CIK classification guidance).

c. Hand Carrying the DTD **and** CIK(s)

Personnel authorized unrestricted access to a DTD and its corresponding CIK may be authorized to hand carry the DTD and CIK, as necessary. The DTD and corresponding CIK must be appropriately packaged and protected separately from each other (e.g., in a separate container or on the local command courier's person). TPI handling of the CIK will be required as follows:

(1) When the same local command couriers will be simultaneously hand carrying the DTD and TOP SECRET CIK,

or

(2) When the local command couriers will be simultaneously hand carrying the DTD and CIK and the TrKEK used to pre-encrypt the TOP SECRET key (designated CRYPTO) in the DTD.

17. **Audit Trail Record Review Requirements:**

a. **General.** The DTD automatically records audit information on the actions performed by the DTD operators. Audit data can be reviewed in either the DTD itself, or by uploading and reviewing it on the LMD. The audit trail uploads must be done when the Audit Icon illuminates. At this point, the audit trail is at least 80 percent full. When the audit trail becomes full, the DTD will display an Audit Trail Full error message, and no further data can be written to the audit trail. Once the audit data has been properly reviewed, uploaded, the DTD audit trail must be reset.

NOTE: Except as indicated in paragraph 17.c (note 3) below, failure to review audit trail data for equipment with audit capability (e.g. DTD, SKL, TKL) when initialized, and/or storing key or issued to a LE within the prescribed time frames will be reported as a COMSEC Incident in accordance with Article 945. Documentation/Retention requirements will be in accordance with Annex T.

b. **Who Should Review.** The audit trail of each DTD storing key(s) must be reviewed by the Supervisory User (or other person designated by the local commander/officer-in-charge) using the Supervisory CIK. The audit trail reviewer should not be a primary user of the DTD, but should have enough knowledge of the authorized user(s) of that DTD and the keying material that the user handles to be able to detect anomalies in the audit trail.

Example of an anomaly:

1. User login indicates May 22, 2002 but then the next transaction logged shows a destruction that occurred on 12 February 2002 with another user login that occurred again on May 22, 2002. Pay particular attention to the information the falls in between one user login to the next attempted user login.

2. DTD audit trail reflects a key issue at 0300 when DTD is maintained in a comms facility operated part-time (i.e., from 0800 to 1600).

3. (Non-watch environment) DTD audit trail reflects segment 22 of key with a daily crypto period was deleted on the 25th but the SF-702 for the container indicates it was opened on the 23rd and 24th (late destruction).

4. (Watch environment) DTD audit trail indicates a segment of key which has a changeover time of 0001Z was destroyed at 1430Z (late destruction)

c. **Frequency of Review.** The audit trail must be reviewed at least once per month although more frequent reviews are encouraged.

NOTES: (1) It is <u>HIGHLY</u> recommended that reviews be conducted NLT the 5th working day of the month following the month in which the material was issued as the material issued to the Local Elements which is superseded will not only be reflected on the LE Working Destruction Report from LCMS but must also be reflected on the account's Consolidated Destruction Report which must be dated NLT the 5th working day of the month following supersession.

(2) In instances where a device is issued on an irregular basis (FLT CINC Communicator), exercise, middle of the month, etc… the audit trail will be reviewed by either a properly cleared, authorized and designated Supervisory user for the LE activity and recorded in an Audit Review Log (if issued for a calendar month or longer) or by the EKMS Manager upon turn-in, whichever

occurs sooner. When authorized LE personnel conduct such reviews, they must be documented in an Audit Review log and retained in accordance with Annex T.

AMD-9

(3) Reviews of DTD, SKL, or TKL audit trail data for devices issued to ~~CMS A&A~~ COR Audit Teams or school houses where the EKMS Manager Course of Instruction (COI) is facilitated are not required unless such is mandated as a matter of local policy by the supporting EKMS account or in ISIC and/or TYCOM directives. Devices used by these entities are restricted in purpose to training functions and is limited to either Test Key or ALC 7 material produced from a non-operational Key Processor (TESTPAC).

d. **Logging Reviews.** The designated reviewer will keep a log of all audit trails reviewed and indicate the following: DTD serial number, date, whether or not any anomalies were detected and name of auditor. These logs will assist the reviewer in tracking any trends or changes in audit information and alert the reviewer to potential security problems. Any potential security problems must be investigated to determine cause.

e. **Classification of Audit Trail Records.** DTD audit trail information in and of itself is unclassified, but is subject to AIS interface flow rules (i.e., whenever audit data is uploaded to a SECRET AIS (e.g., LMD/KP) and/or saved to removable media (e.g., a floppy disk) for later review by supervisory personnel, the data, and any removable media it may be stored on, must be classified SECRET.

f. **Retention of Audit Trail Review Logs.** Audit trail review logs will be retained for at least two years. A sample DTD/SKL Audit Trail Review/Reinitialization log can be found on the NCMS CAS portal.

18. DTD *Interface Flows*

a. **DTD as a common fill device:** Interface flows involving key/key tag and application software flows are not subject to computer security (system-high) rules. These flows are trusted to occur at their actual intended classification level. The fill device application program provided with the DTD is unclassified. The audit trail records created by the fill device application program are also unclassified until uploaded to a computer and/or stored.

b. **DTD use with an Automated Information System (AIS) (e.g.,**

LMD/KP): Interface flows between the DTD and AISs are **not** subject to computer security (system-high) rules. This includes any User Application Software (UAS) and audit data either uploaded or downloaded from a classified computer (e.g., LMD). For example, if UAS is downloaded from a LMD (Secret-high AIS) to the host side of a DTD, the DTD will **not** be classified on the basis of that connection/interface flow.

19. **DTD Zeroization & Sanitization**

a. When activated, the DTD's zeroization function will sanitize all data, destroy all stored key, and delete all CIKs from the DTD. (The zero function will not delete application software from the DTD, nor will it delete audit records from the DTD).

b. Regardless of its handling requirement before zeroization, once the zeroization function is successfully completed, the DTD is UNCLASSIFIED CCI. The operator can only treat the DTD as zeroized if the display shows the "zeroization complete" message. If this message does not appear, a depleted battery may be the cause. Install a fresh battery and press the [ZERO] key the correct number of times to verify that the display message "zeroization complete" appears. If the message still does not appear, then it must be assumed that zeroization is not possible due to a malfunction. The battery must be removed from the DTD and the DTD must be protected according to its classification (see paragraph 8 for classification guidance) until it can be turned-in to a depot and repaired.

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

20. **Supervisory User Responsibilities**

a. Create CIKs and ensure that the number of CIKs created are kept to the minimum required to satisfy local operational requirements.

b. Ensure each CIK has a serial number to support its accountability in DTD audit trail records. The serial number will be created and assigned by the Supervisory User in strict accordance with paragraph 7.c. When creating CIK serial numbers, the Supervisory User will ensure that the CIK serial number is unique from those for all other DTD CIKs associated with the AIS or LMD which reviews his/her DTD's audit trail.

c. Establish procedures that ensure that an accurate determination can be made regarding which individual user(s) had access to a CIK at any given time.

d. Re-initialize CIKs at least annually and whenever key compromises occur.

e. Always store Supervisory CIKs separately from associated DTDs.

f. Ensure DTDs, which are initialized and/or storing keying material, are examined for breaches in housing at least weekly.

g. If designated by local Commander/Officer-in-charge to be audit trail reviewer, review audit trail records as required by this document.

h. **Promptly report** CIKs that are suspected of having been copied (i.e., when CIK update count check reveals disparity between update count on DTD and update count on the CIK) and review audit records to determine whether CIK was copied and what unauthorized actions, if any, were performed with the copied CIK. If review results confirm that CIK was copied, notify your EKMS Manager immediately so that a COMSEC incident report may be prepared and forwarded as required by paragraph 26.

i. Ensure a tag is attached to each CIK (e.g., via a chain) that minimally identifies the CIK's classification and serial number.

j. Ensure that a tag is attached to each DTD, via the lanyard ring, that indicates the classification of the DTD when its associated CIK is not inserted. Example: If the DTD is storing classified information on the host side, the DTD will be classified even when its associated CIK is not inserted.

k. Ensure that procedures are implemented to zeroize any DTD prior to its being taken out of use. This will delete all data on the host side and destroy all key associations with the CIKs. It does not delete the DTD operating software, UAS, or audit data. The audit data should be uploaded before the DTD is taken out of service, and it must be deleted from the DTD.

21. **Operator Responsibilities**

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

b. **Promptly** notify the Supervisory User/EKMS Manager of any DTDs storing key and CIKs that are not tagged as described under Supervisory User Responsibilities.

c. Examine DTDs for casing damage or cracks at least **weekly or upon next opening of the security container for a non-watch environment.**

d. Be familiar with the handling and safeguarding requirements of this doctrine and report all violations of same to the Supervisory User/EKMS Manager.

22. **EKMS Manager Responsibilities for User Application Software**

a. Ensure that only NSA cryptographically signed application software is installed in the DTD.

b. Maintain records of all UAS installed in each DTD charged to the account. These records will identify the DTD by serial number and the UAS installed in that DTD. In the event a DTD malfunctions, requiring turn-in to a CRF for replacement, these records will ensure that replacement DTDs (swap-out units) arrive with the required UAS installed.

23. **Use of the DTD & STE for Over-the-Air Key Distribution**

Use of the DTD and STE is the preferred, authorized method for transferring key for limited duration operations. The DTD and STE can be used to rekey units in the field who have telephone access as well as aircraft crews who may have landed at airports other than their own base. This can preclude carrying excessive amounts of paper material, especially if they plan an extensive number of days away from home base.

An NSA-approved adaptor/connector **must** be used to connect the DTD to the STE data port for purposes of passing key over STE secured point-to-point circuits.

Also see Chapter 11, Article 1165.e.

24. **OTAT of DTD TrKEK**

a. DTD TrKEK is generated by Electronic Key Management System (EKMS) KPs and is used to encrypt key transfers from a LMD/KP to a DTD. Most TrKEK is loaded into the DTDs of Local Elements (LE) by supporting (parent) LMD/KP accounts. This keying procedure requires the physical return of the DTD to the supporting LMD/KP.

b. E-Fill software versions later than 409 (e.g., 410, 411, 5.4, etc.) eliminate the need for the DTD to be physically returned to the LMD/KP for new TrKEK. These later versions are capable of supporting routine (non-emergency) OTAT of new or replacement DTD TrKEK between communicating DTDs.

c. Users of E-Fill versions 4.10 and later will comply with these provisions when OTATing new or replacement DTD TrKEK:

(1) Sending LMD/KP must implement "E-Fill 410/411/5.4" protocol.
(2) Transmission must be secured by STE. Routine (non-emergency) OTAT by other OTAT-capable equipment (e.g., KG 84, KIV 7, etc.) is not authorized.
(3) Receiving site must have at least two DTDs that hold different TrKEKs. New TrKEKs for one DTD may be transferred via OTAT to the other DTD and vice versa.

d. LMD/KPs that implement E-Fill 410/411/5.4 protocol may deliver TrKEKs via OTAT on circuits/nets that are secured by DTD TrKEKs or via point-to-point circuits and multi-station nets that are secured by a STE.

25. **Emergency Protection**

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

26. **Reportable COMSEC Incidents**

a. The following incidents are specific to the DTD and are intended to supplement those general COMSEC incidents and practices dangerous to security (PDS) identified in Chapters 9 and 10:

(1) Loss of a DTD.

(2) Loss of a valid DTD CIK when the associated DTD has not been; stored properly, under the direct control of authorized personnel **or** failure to delete a lost/stolen CIK from its associated DTD. If not protected as described or the lost CIK is not deleted from the DTD, all key and host side data protected by the CIK must be assumed to be compromised. See 26.c.1 and 26.c.2 below for additional information. (reportable to the CONAUTH for the key).

(3) Unauthorized copying of a valid CIK[12]

(4) Unauthorized access to a CIK or DTD.

(5) Storage of key on the host side of DTD.

(6) Loss of TEMPEST integrity because of failure to detect a breach in the DTD's housing.

(7) Unauthorized extension of a Storage Key Encryption Key (SKEK) cryptoperiod. (DTDs in-use/issued must be reinitialized annually when used to store/protect key **and documentation of such must be on file**). This is not applicable to devices which have not been initialized (in the box or stored at the Managers level and not protecting key)

b. Follow reporting guidance in Chapter 9.

c. Compromise Recovery Actions for Lost CIK/Lost DTD.

(1) If a CIK is lost and the DTD has not been outside of proper storage or the direct control of an authorized user, promptly delete the lost CIK from its associated DTD, report it to the Supervisory User or EKMS Manager, as applicable and document it locally as a non-reportable PDS.

(2) If a DTD is lost, promptly zeroize/destroy its associated CIK(s) and report the loss in accordance with Chapter 9. In the report of loss, describe the degree of protection afforded all associated CIKs when the DTD was first discovered missing. If the DTD's associated CIK(s) were not lost or compromised, but remained under the protection required for their classification (e.g., TPI), the user key and TrKEK that were

[12] 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 **before** the original CIK is used.

stored in the lost or compromised DTD need not be superseded. Any classified host side data stored in the lost or compromised DTD must be considered compromised.

27. **DTD Repair & Maintenance**

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

PART II

Definitions Unique to DTD Safeguarding and Handling Policy

Audit Trail Records - Chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event.

Classified CIK - A CIK that can be used to output classified (unencrypted) key designated CRYPTO from a DTD.

Crypto Ignition Key (CIK) - The information contained in a key storage device (KSD) that is used to electrically lock and unlock the secure mode of crypto equipment. When the KSD containing a CIK is inserted in the DTD and the DTD is powered on, the cryptographic capabilities of the DTD are unlocked to allow for the input/output and handling of key and other information. There are two types of DTD CIKs: User CIKs and Supervisory CIKs.[13]

Data Transfer Device (DTD or AN/CYZ 10) - The DTD provides cryptographic security for the storage and transfer of all types of key, and protective storage for related data (e.g., key tags and audit data) and other data depending on the application software in the DTD. Other newer electronic storage devices such as the Secure Data Transfer Device 2000 (SDS) and the Simple Key Loader (SKL) are also referred to as next generation Data Transfer Devices (DTDs)

Host Side (with regard to DTD) - Part of the DTD that performs no cryptographic function. The Host Side is used to store and execute application software and store unencrypted data.

Initialized CIK - A CIK that has gone through the randomization process and is now associated with a particular DTD to allow access to that DTD. It has a specific SKEK associated with that CIK, and will only allow specified access to classified key loaded by that CIK.

Interface Flows - The DTD can interface with other equipment for four different purposes: transmit or receive key, receive software, transmit audit records, and transmit or receive host-side data. Each of these is called an "interface flow."

[13] In addition to controlling access based on supervisory versus operator privileges, the DTD's CIKs can also be used to control access to key stored in the DTD's key storage database. The DTD's key storage database can be segregated, with access to the key granted only to users with associated CIKs.

Keyed DTD - DTD that may or may not contain user key and/or Transfer Key Encryption Key (TrKEK) and has its associated CIK inserted. Also see Unkeyed DTD.

Storage Key Encryption Key (SKEK)[14] - Key used internally by the DTD to encrypt keys stored in the DTD's key storage database. Where the DTD's key storage database is compartmented, there is a unique SKEK per compartment. The SKEK generated in the DTD has a one-year cryptoperiod.

Supervisory CIK - Has all the privileges of the User CIK and, in addition, allows the Supervisory User to perform utility functions such as loading application software and uploading and reviewing audit trails. Also see User CIK.

Supervisory User - Individual designated by CO/OIC to create CIKs, assign serial numbers to them, and to fulfill additional responsibilities for their handling and safeguarding (see paragraph 20). The Supervisory User and EKMS Manager/Local Element (Issuing) may be one and the same.

Tactical Key - Traffic encryption key (TEK), key encryption key (KEK), or transmission security key (TSK) intended to secure information or data that is perishable, has low intelligence value (i.e., low national or international sensitivity), and is classified no higher than Secret.

Transfer Key Encryption Key (TrKEK) - Key used in the DTD to decrypt previously encrypted user key (loaded into the DTD as encrypted key) to enable the DTD to output user key in unencrypted form.

Unkeyed DTD - DTD that may or may not contain user key and/or TrKEK and does not have its associated CIK inserted. Also see Keyed DTD.

User CIK - Allows the DTD operator to perform all the basic key handling and distribution functions of the DTD. Also see Supervisory CIK.

User Key - Key which has been loaded into the DTD for storage and subsequent transfer to other cryptographic devices, equipment, or systems.

[14] Also known as Local Key Encryption Key (LKEK).

ANNEX AA

SAMPLE MESSAGE ADVISING NCMS OF NAVY EKMS ACCREDITATION

The following is a sample message advising NCMS that all requirements for Navy EKMS accreditation have been completed. See Article 405.h.(6) for details concerning this requirement.

FM (INSERT COMMAND TITLE HERE)
TO NCMS WASHINGTON DC
INFO ISIC
ADMINISTRATIVE CHAIN OF COMMAND
SPAWARSYSCEN ATLANTIC CHARLESTON SC
BT
UNCLAS //N02280//
MSGID/GENADMIN/COMMAND/-//
SUBJ/NAVY EKMS ST&E CERTIFICATION//
REF/A/DOC/NCMS WASH DC/-//
REF/B/LTR/COMUSFLEETCYBERCOM/23MAY2012//
REF/C/DOC/SPAWARSYSCEN ATLANTIC MEMO/-//
NARR/REF A IS EKMS-1 (SERIES). REF B IS US FLEET CYBER COMMAND’S AUTHORITY TO OPERATE (ATO) LETTER FOR THE DON EKMS PHASE 5 TIER 2. REF C IS THE SPAWARSYSCEN ATLANTIC ST&E CERTIFICATION QUESTIONNAIRE.//
POC/SAILOR, J.D./CTOC/USS NEVERSAIL/TEL:312-668-1291/EMAIL: SAILOR(AT)NEVERSAIL.NAVY.MIL//
RMKS/1. IAW REFS A AND B, NAVY EKMS ACCREDITATION REQUIREMENTS SET FORTH IN REF C WERE COMPLETED ON (YYMMDD).//

ANNEX AB

CHECKLIST FOR SECURE TELEMETRY MISSLE FIRINGS

NOTE: Missile firings are no longer reportable as COMSEC incidents. Commands must instead forward information concerning missile firings in strict accordance with this Annex.

EKMS managers will notify their Commanding Officers/Officers in Charge of this requirement and work with command personnel to ensure that this information is completed and forwarded to DIRNSA//I2S// within 30 days of the launch of a missile using secure telemetry:

1. Laboratory checkout/calibration:________________________
____

   Date completed:____

   Location of data:______________________________________

2. Test item:____

3. Location of test:______________________________________

4. Type of keying material used:__________________________

5. Short title/edition/segment:___________________________

6. Holding battery installed (date):______________________

7. Keying material loaded: (date):________________________

8. Test date:____

9. KG-66/KG-66A/KGV-68/KGV-68B serial number:_____________
(Note: The serial number is only required for KG-66/KG-66As. For KGV-68/KGV-68Bs which are ALC 2 insert NA for the serial number.

10. Test item KG-66/KG-66A/KGV-68/KGV-68B extended (approx. time):____

11. Approximate location of impact:________________________
____

12. Recovery attempt made (YES, NO). If NO, provide explanation:____

13. Transaction number to relieve the EKMS account of the accountability for the fired missile:__________________

14. Reported to EKMS Manager (date/approx. time):__________
____

15. Problems encountered (if none, so state):______________
____

16. Report submitted to COMSEC Custodian (date):___________

17. Report submitted to DIRNSA//I2S// (date):______________

18. Report submitted by: __________________________________
(include full name, rank/grade, office code/position at command, and office phone number)

NOTES: 1. When filled in and depending on mission, a minimum classification of CONFIDENTIAL must be assigned.

2. EKMS Manager must be notified of missile firings so as to ensure that appropriate accounting adjustments are made to the EKMS account command's inventory (e.g.,SF-153 Relief from Accountability).

3. Checklist information may be mailed to DIRNSA//I2S// using methods approved in this manual for the classification assigned to the document (a minimum of CONFIDENTIAL), or submitted via naval message having a minimum classification of CONFIDENTIAL. If mailed, include NCMS//N5// as a copy to addressee; if submitted by message, include NCMS//N5// as an information addressee.

ANNEX AC

TALON CRYPTOGRAPHIC TOKEN (TCT)

1. **Purpose and applicability**: To promulgate guidance related to the procurement, training, safeguarding, handling, storage and accountability of the TALON Cryptographic Token (TCT). The use of the terms KOV-26, TCT, or TALON card refers to the same device. Additional information, if necessary can be found in the System Security doctrine at: http://iad.nsa.smil.mil

2. **Description/Use**:

a. The TCT is an ALC 1 item designated as a Controlled Cryptographic Item (CCI) and is continuously accountable to the Central Office of Record (COR) by serial number. The Short Title associated with the TCT is KOV-26.

b. KOV-26s are Type 1 encryption devices designed to provide wired or wireless secure voice and data connectivity through the combination of the functionality of an Inline Network Encryptor (INE) supporting Internet Protocol (IP) operations over commercial networks with a Secure Communications Interoperability Protocol (SCIP) terminal. KOV-26s can use either Pre-Placed Keys (PPKS) and FIREFLY/Enhanced FIREFLY (FF/EFF) keys and are interoperable with either High Assurance Internet Protocol Encryptor Specification (HAIPE/IS) version 1.3.5 or SCIP 210/230.

c. Configuration, installation assistance, status and help menus are available through the TALON Host Software (THS) for supported user types which are either: End Users and Site Security Officers (SSOs).

d. The KOV-26 (TCT) provides message confidentiality and access security controls up to TS/SCI with a maximum data throughput of 5Mbps or 230 Kbps for IP and SCIP traffic, respectively.

e. The KOV-26 high assurance cryptographic token is housed in a Type II extended Personal Computer Memory Card International Association (PCMIA) card bus form factor and provides Type 1 algorithms for key management, encryption, identification and authentication.

f. The KOV-26 uses a CIK-equivalent logon authentication in lieu of a physical CIK. The KOV-26 recombines; the CIK-split data, possession of a host computer holding the matching CIK-split data and knowledge of either the End User or SSO password facilitate authentication.

g. Communications are possible via one of four Commercial Off-The-Shelf (COTS)USB network adaptors referred to as the TALON Communicator Adaptor (TCA). These include; (1) Ethernet (RJ-45/802.3), (2) Wi-Fi (802.11b/g) Wi-Fi Protected Access or Wired Equivalent Privacy (WPA/WEP), (3) Modem (v.90/56Kbps) supporting both HAIPE and SCIP voice or data via dial-up Public Switched Telephone Network (PSTN) and (4) Serial/RS-232 adapter supporting SCIP voice and data via Integrated Services Digital Network (ISDN) or narrowband satellite terminals.

h. The internal, non-replaceable battery associated with the KOV-26 has an estimated five to seven year lifespan.

3. **Site Security Officer (SSO) (Responsibilities):** SSOs must possess a security clearance equal to or higher than the highest classification of keying material loaded into any KOV-26s managed and is responsible for adhering to local IA security policies. The SSO may be the EKMS Manager and up to three SSO accounts may be created per KOV-26. If the SSO is also the EKMS Manager, the individual must have a clearance equal to or higher than the Highest Classification Indicator (HCI) of the account. Specific duties of the SSO include but are not limited to;

a. Establishment of SSO and End User accounts and assignment of End User privileges. Up to a maximum 15 End User accounts can be established by the SSO.

b. Establishment and configuration High Assurance Internet Protocol Encryptor (HAIPE) network settings. This includes; working with the Network Administrator to define network destinations in which the End User is authorized to communicate and configuring the KOV-26 with, IP addresses, Domain Name Server (DNS) addresses or other HAIPE traffic settings.

c. Loading and assignment of keying material, the entering of effective date data and establishment of the association of keying material with the appropriate encryption algorithm. This also includes the assignment of the keys for either HAIPE or Secure Communications Interoperability Protocol (SCIP) usage.

d. Assignment of end user privileges. This includes but is not limited to; the ability to load/delete keys, loading of software, use of the TALON Communication Adaptor (TCA), the ability to perform rekeys, the use of SCIP/HAIPE protocols and the setting of SCIP voice or data security levels.

e. Documenting and maintaining a list of both SSO accounts and End Users associated with a KOV-26 by serial number. The SSO or End User account(s), as applicable must be deleted when the respective individual transfers, retires, separates or no longer requires access.

4. **EKMS Manager (Responsibilities)**: Is responsible for the duties and responsibilities outlined in Article 455. Additionally, with regard to the KOV-26/TCT, the EKMS Manager or Alternate may also be the SSO.

5. **Software and Limitations**: The TALON host software (THS) provides a Graphical User Interface (GUI) for configuration and management functions for either the End User or SSO. The THS-End User and THS-SSO **cannot be** loaded on the same host computer.

6. **Field Software Upgrades (FSUs)**: Unless otherwise prohibited, consistent with this annex and local IA policy, FSUs may be performed by either the EKMS Manager/Alternate, SSO (if appointed) or End User.

Only encrypted images received via a trusted distribution path are authorized for use in performing software upgrades.

Approved TALON Card software upgrades can be obtained from: https://www.iad.gov/SecurePhone/index.cfm

7. **Classification**:

a. Following activation by an SSO in either the Initialized or Configured State, the TALON card is classified based on the highest classification of key filled in the device when the device is; (a) in the configured state and (b) a user is logged on/has authenticated to the device.

b. When in the; Boot Only State, Programmed State, SSO Default State, Initialized State, Unrecoverable State or Configured State the device is unclassified CCI.

c. The device must be safeguarded, stored and handled in accordance with Chapter 5.

> **NOTE: Unrecoverable refers to a transient state that is entered when a tamper condition is detected. This state results in zeroization of the card, JK0 and a device reset. If the integrity of the RP software is verified, the device will transition to the Programmed State but must be returned to the vendor for inspection, retest or reload of JK0. The movement of TALON cards will be documented following either proper local custody or transfer procedures outlined in Chapter 7.**

8. **Transitional States**:

a. When in the SSO default state, the Initialized State or Configured State; if directed to zeroize by either the End User or SSO, the KOV-26 transitions to the SSO Default State and destroys all; key, as well as both the SSO and End User ID/Host entries.

b. When in the SSO Default State, the Initialized State or Configured State; if directed to sanitize, the KOV-26 transitions to the Boot Only State and destroys all; key, classified software, initial keying material and both the SSO and End User ID/Host entries.

c. When in either the Initialized or Configured State and all three SSO ID/Host ID entries are locked out, the KOV-26 transitions to the SSO Default State and destroys all; key, as well as both the SSO and End User ID/Host entries.

> **NOTE: Six unsuccessful login attempts will result in an account lockout. An illustration of both the lifecycle and transitional states of a KOV-26 can be found in Figure AL-1.**

9. **Access and Responsibility Acknowledgement**:

a. Access to either keyed TALON cards or keying material for loading such devices is restricted to personnel meeting the requirements reflected in Article 505.

b. TALON cards will not be issued to contractors from a Department of the Navy (DON) EKMS account without, in addition to requirements stated in this Annex compliance with the applicable provisions set forth in OPNAVINST 2221.5(series) and Articles 505.f and 505.g, as applicable.

c. Access by foreign nationals must have prior approval from NSA//DP02 and/or the Controlling Authority, as applicable Article 505.

d. Personnel performing TALON card configurations as part of a system-wide or organizational deployment through the GUI interface of a client PC do not require either written access to keying material or execution of a SD Form 572 ~~COMSEC Responsibility Acknowledgement form~~ unless the individual's duties require access beyond this extent to such material. AMD-9

10. **Validation of requirements**: Will be per Article 610.

11. **Password Security**:

a. Consistent with other devices, i.e. LMD/KP, OMNI, etc… passwords will be classified and safeguarded based on the highest classification of keying material loaded in the TALON card, when keyed.

b. Password lengths will be consistent with current DoD strong password requirements at the time of issue. The length or complexity of passwords may increase or change, as applicable, as directed by DoD or higher policy when so stipulated.

c. Passwords must contain a combination of letters, numbers, special characters and consist of both upper and lower case.

d. Passwords must be changed at a minimum of every 60 days or sooner, if so directed by higher authority (e.g., Computer Task Orders (CTOs)).

e. If passwords are recorded, such will be restricted to in the form of a SF-700 which will be labeled, handled, stored, safeguarded and inspected in accordance with Article 515.f.

f. Passwords must be communicated to End Users or SSOs in person or distributed via an approved secure circuit(STE or SIPRNET).

g. Upon receipt of the password, the End User or SSO must change the password to a new unique one meeting the requirements stated above.

h. Six successive failed logons will result in the KOV-26 deleting its CIK-split data for that End User or SSO account, as well as lockout of the User ID/Host ID combination.

12. **Keying Management (Types of Key Used, Ordering, Forms, Distribution, Loading, and Management)**: Unlike traditional keying material which is auto distributed based on an accounts validated allowance and distribution profile, keying material for use in TALON cards is considered modern key and MUST be ordered by EKMS Managers.

a. Types of key used:

1. **HAIPE Pre-placed key (PPK)**: PPKs may be loaded prior to their effective date but must match the security level configured in the HAIPE traffic settings. An algorithm (BATON or MEDLEY) and effective date must be assigned prior to use for traffic. Up to 348 PPKs supporting up to a maximum of 32 security associations for up to 12 months each can be held by the KOV-26.

2. **HAIPE FF/EFF Vector Sets**: Are only used during a FF/EFF exchange to generate a Traffic Encryption Key (TEK). FF/EFF vector sets used to generate a FF/EFF TEK between peer devices must have the same; universal, classification and partition code. The same FF/EFF vector set may not be filled into two HAIPE devices as each FF/EFF vector set must have a unique Keying Material Identification Number (KMID). Up to 8 FF/EFF keys representing 8 universals (current + future editions) up to one-year can be held by the KOV-26.

3. **SCIP FF/EFF Vector Sets:** Are only used during a FF/EFF exchange to generate a FF/EFF TEK between peer devices must have the same; universal, classification and partition code. The same FF/EFF vector set may not be filled into two SCIP devices as each FF/EFF vector set must have a unique Keying Material Identification Number (KMID). Up to 4 SCIP FF/EFF keys representing 4 universals (current + future editions) up to one-year can be held by the KOV-26.

4. **FF/EFF Generated TEK**: Session based keys generated during a key exchange between either HAIPE or SCIP devices to encrypt/decrypt traffic.

5. **SCIP Seed Key**: Must be converted to operational key prior to use.

NOTE: Classroom training will make use of Unclassified Test Key only. Such may be used indefinitely and does not have regular effective/supersession dates like that associated with operational keying material.

b. **Ordering:** Will be typically performed by the EKMS Manager or Alternate but in either case the individual ordering modern key must be privileged to place such orders as reflected in the accounts User Registration data on file at the EKMS Central Facility (CF). Keying material may be ordered either by; faxing the request to the EKMS CF, via the LMD/KP or through the interactive online-ordering function located at the URL in 15.b below.

NOTE: For additional information regarding the establishment of privileges for ordering modern key, see Annex AE.

c. **Forms**: Order forms for TALON cards, as well as guidance on establishing key order privileges can be found at: https://www.iad.gov/Keysupport/index.cfm

d. **Distribution**: Modern keying material is delivered to requesting and authorized accounts via the X.400 message server associated with the LMD/KP.

e. **Key Loading**: Will be performed by the EKMS Manager, Alternate or LE Issuing, as applicable via a DTD, SDS, or SKL using a TALON Fill Cable (TFC).

NOTE: TPI handling and storage requirements set forth in Article 510 must be adhered to when loading Top Secret keying material from a DTD, SDS, or SKL.

f. **Key Management**: It is highly recommended that EKMS Managers maintain either a spreadsheet or database to record TALON card key loads reflecting KMIDs and device serial numbers. Alternatively, the data can be reflected in the remarks or comments field of the SF-153 used to issue the TALON Card from LCMS. If the device is lost, stolen or otherwise compromised, the EKMS Manager will provide the KMID and TALON Card serial number to the EKMS CF to have the KMID added to the Compromised Key List (CKL) database at NSA.

g. **Key Destruction**: Individual or multiple-keys loaded in a can be zeroized in accordance with procedures in the devices user manual. An Active Zeroization is accomplished through clicking on the zeroize icon in the GUI interface of either the End User or SSO THS application whereas a Panic Zeroization is accomplished by bending the steel portion of the card, when unpowered.

h. **Key Rekey**: In view of the one-year cryptoperiod associated with TALON card keying material (HAIPE FF/EFF Vector Set or SCIP FF/EFF Vector Set), the device must be rekeyed at a minimum of annually. Instructions for performing electronic rekeys can be found at: https://www.iad.gov/KeySupport/index.cfm under the "Equipment Rekey" tab.

TALON Card Electronic Rekey Numbers

U.S. Users	Toll Free	1-800-218-3238
	Comm.	1-410-526-3444
	DSN	312-238-4444
CF Assistance	Toll Free	1-800-635-5689

NOTE: To perform a rekey, the person must be privileged by the SSO with both the Load Key and Modem privilege.

16. **Issuance and Accountability of TALON Cards**:

a. All TALON card local custody transactions will be handled by the EKMS Manager/Alternate or LE Issuing, as applicable and accomplished following proper local custody procedures set forth in Article 769.

b. EKMS Managers must ensure that personnel issued TALON cards are appropriately cleared and authorized such access in accordance with Article 505.

c. Local custody documents for the issuance and return of TALON cards will be retained in accordance with Annex T.

d. TALON cards will be inventoried at a minimum in accordance with Articles 766, 775 and 778 as applicable.

17. **Protective Technologies**: Although tamper labels cannot be applied to the KOV-26, the device is protected by a Tamper Boundary that will trigger zeroization upon damage or opening of the metal casing. Evidence of tampering must be reported in accordance with Article 945.

18. **Alarm Conditions**:

a. May be cleared through ejecting the card, rebooting the host computer and reinsertion of the card.

b. If the alarm persists, a visual inspection must be conducted.

c. If tamper is detected, report the matter in accordance with Article 945.

19. **Audit logs**:

a. Are unclassified but may be sensitive. Local policy may dictate that the logs contain classified data and require marking, safeguarding and disposal in accordance with local policies and SECNAV M5510.36.

b. Will be reviewed by the EKMS Manager or SSO (if designated) when the LED or card indicates the log is 80% full or monthly, **whichever occurs sooner.** The EKMS Manager must ensure that logs are; created, used, maintained and retained for 2 years.

> **NOTE:** Once the log reaches 98%, the log begins to overwrite 2% of the oldest entries which could hinder auditing. **It is highly recommended that local policy, as well as Letters of Agreement specifically address who is responsible for performing these reviews and address both documentation and retention requirements.**

c. Failure to conduct and document audit trail reviews and retain logs of such as stated above will be reported in accordance with Article 945.

20. **TEMPEST:** The KOV-26, when installed in a laptop designed to accommodate a PCMIA Type II card bus card has passed applicable TEMPEST standards. TEMPEST standards will not be met if installed in a laptop or host computer that, by itself, exceeds TEMPEST requirements. If necessary, organizations deploying TALON cards should consult with a Certified TEMPEST Technical Authority (CTTA) from SPAWAR N723. Contact data is available on the https://infosec.navy.mil web site.

21. **Shipping**:

a. TALON cards will be shipped in accordance with Article 535.

b. Unlike legacy COMSEC equipment or equipment which permits key extraction, TALON cards may be shipped in either a keyed or unkeyed state. However, when keyed the secure mode must be disabled.

c. Under no circumstance will passwords or PINs be shipped with the associated equipment.

22. **Procedures for Failed TALON Card Devices**: Users experiencing problems with issued TALON cards will request assistance from the SSO, LE Issuing or EKMS Manager, as applicable.

a. Either the End User or SSO can cycle the power to clear the error condition or swap the TCA with a known good unit in an attempt to isolate the problem.

b. If the alarm status clears, the End User or SSO should conduct a review of the audit log to determine the cause of the alarm.

c. If the actions above do not resolve the issue and the device is found to be defective it will be returned following proper local custody procedures set forth in Articles 712 and 769 of this manual.

d. All other maintenance actions will be performed by the vendor for the device.

e. EKMS Managers must follow applicable procedures in EKMS-5 Chapter 4 in requesting disposition instructions for failed units.

NOTE: If the keying material cannot be zeroized, the device will be shipped based on the highest classification of key possibly still in the device at a minimum Secret level.

23. **Emergency Actions**: In the event of either an impending site overrun or capture, zeroize the KOV-26. Then, as time permits, if a THS workstation is available zeroize the unit or bend the steel portion of the card over a sharp edge inducing a tampered state.

24. **Reportable COMSEC Incidents Unique to the TALON Card** : The loss, theft, unauthorized access, evidence of tampering, unauthorized maintenance, attempted maintenance or unauthorized shipment (shipment not coordinated with or conducted by the EKMS

Manager/Alternate, or LE Issuing, as applicable) of a TALON card must be reported in accordance with Article 945.e.

a. **Additional device specific COMSEC Incidents:**

1. **Password Compromise:** In addition to reporting of such as a COMSEC Incident, all cards must immediately have the SSO or End User passwords, as applicable associated with card(s) changed.

2. **Loss or Compromise of a PPK:** Such reports must also include the applicable KMID and state whether any compromised End User or SSO passwords involved.

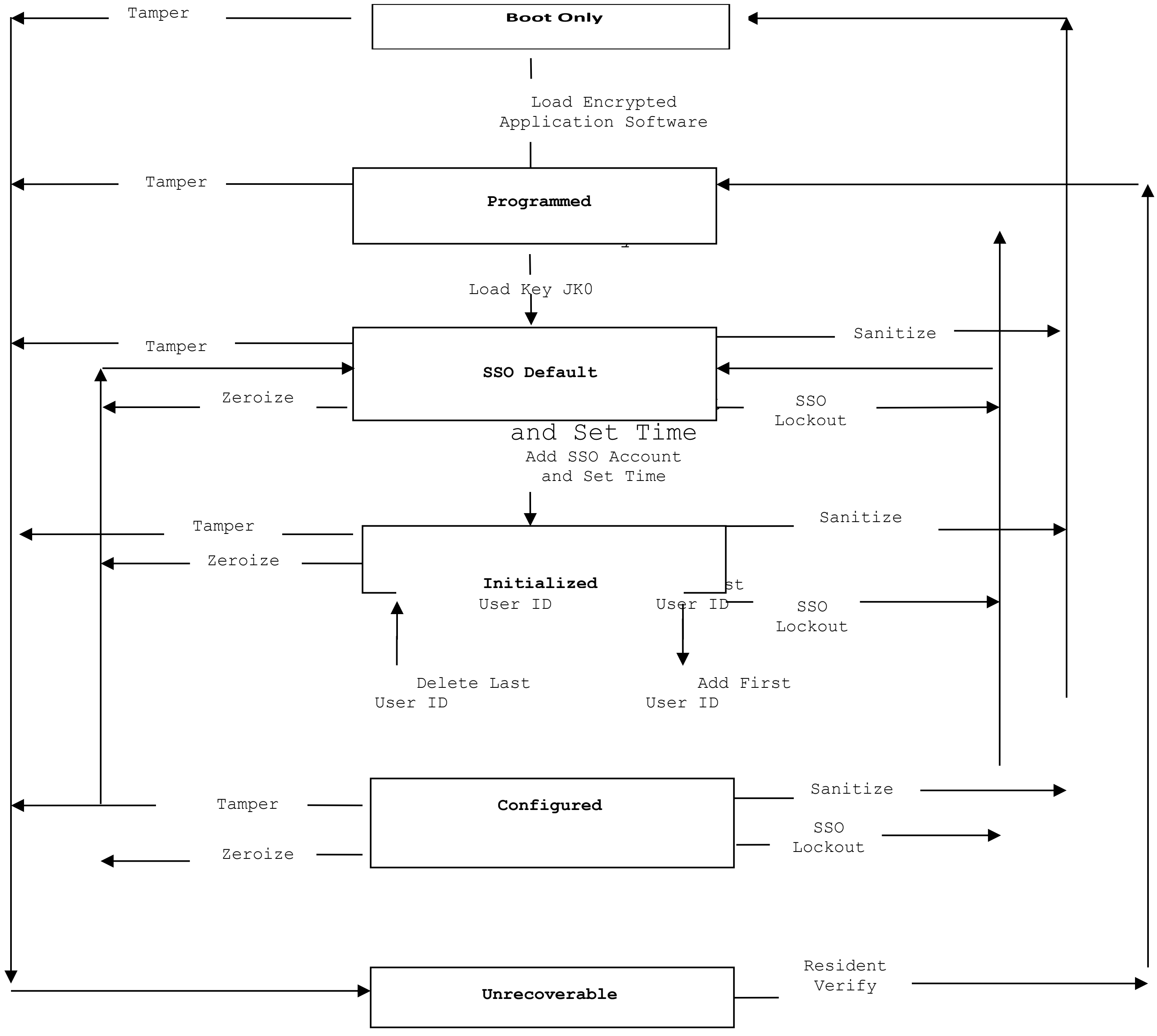

Boot Only
Tamper
Load Encrypted Application Software
Programmed
Tamper
Load Key JK0
SSO Default
Tamper
Zeroize
Sanitize
SSO Lockout
and Set Time
Add SSO Account and Set Time
Initialized
Tamper
Zeroize
Sanitize
SSO Lockout
User ID
User ID
st
Delete Last User ID
Add First User ID
Configured
Tamper
Zeroize
Sanitize
SSO Lockout
Unrecoverable
Resident Verify

FIGURE AC-1

ANNEX AD
SECURE TERMINAL EQUIPMENT (STE)/ASSOCIATED KSV-21 CARD AND IRIDIUM SECURITY MODULE (ISM)

1. **Scope and Applicability**: This Annex contains minimum security requirements for the protection, handling, accountability, and use of the KSV-21 cryptographic card associated with the Secure Terminal Equipment (STE). The capabilities discussed herein are offered in the Release 2.x software for the STE. Any waiver requests from this policy will be addressed to NCMS//N5// for consideration.

This Annex cannot address every conceivable situation that might arise in the day-to-day operation of an account. When unusual situations confront the EKMS account manager, Local Element (Issuing), or users of STE COMSEC material, the basic tenets of physical security and proper accounting controls, coupled with good judgment and common sense, will protect the COMSEC material until instructions or guidance can be received from NCMS//N5// or the EKMS CF.

The Iridium Security Module (ISM) operation with the Iridium 9505 satellite handset is addressed in TAB-1 of this Annex.

2. **Introduction to 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). The STE consists of a host terminal and 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. The speed and quality available on ISDN enables the STE to offer quality secure voice and significantly faster data rates than previous secure telephones. In addition, the STE offers advanced features such as secure voice conferencing and fast auto-secure negotiation with other STEs on ISDN services. When the cryptographic card is removed, the STE can still function similarly to a commercial desk set and provide non-secure communication services. A tactical version of the STE provides connectivity to tactical communication systems such as the Mobile Subscriber System (MSS) or Tri-Service Tactical Communications System (TRI-TAC) switches. With the addition of the optional Future Narrow Band Digital Terminal

(FNBDT) protocol, the STE will be able to negotiate secure sessions with future digital wireless handsets and other FNBDT products.

b. **KSV-21 Card**: 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 Electronic Key Management System (EKMS) Manager. When necessary, the credential of the individual binding to the cryptographic keys can also be programmed and stored. The KSV-21 card is built with many anti-tamper technologies, one of which is the Crypto-Ignition Key (CIK). Initially, the KSV-21 card is programmed with a complete CIK. While in this state, the KSV-21 card is known as a fill card. During the card association with a STE, the CIK is split and a component of the CIK is transferred to the STE for storage. This process converts the fill card into a user card. Subsequently, each time a correct user card is inserted in the STE, the CIK component in the STE is transferred back to the card and restores the CIK, which enables the card security services. The CIK is updated each time the card is inserted and removed from the STE to prevent the CIK from being duplicated. It is advisable to make a backup of each user card to retain the information in case zeroization occurs.

(1) When inserted in a STE, the KSV-21/STE system is classified and must be protected to the highest security level that the KSV-21/STE can achieve. 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 present to observe the STE.

(2) With appropriate cryptographic keying material in the KSV-21 card, the combination of KSV-21 and STE have 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 SCIFs.

3. **National Security Agency (NSA):** The National Security Agency is the executive agent for national level policy affecting COMSEC material. NSA is also responsible for the production of most COMSEC material used to secure communications as well as for the development and production of cryptographic equipment. NSA operates and maintains the Electronic Key Management System (EKMS) Central Facility (CF) for STE keying

material and serves as the Controlling Authority for all STE keying material.

4. **Terminal Privilege Authority (TPA) Responsibilities:**

a. **TPA responsibilities will reside with the EKMS Manager/User Representative (UR) or a designated STE Material Control User (MC User).** STE MC Users at the LE (Issuing) level will be designated in writing by the Commanding officer and must adhere to the same responsibilities previously required of a STU-III MC User in accordance with this manual and local command instructions. Designation of a STE MC User is at the EKMS numbered account Commanding Officers discretion.

b. TPA manages the features and capabilities of the STE for other users, including software upgrades for the STE and KSV-21 cards when necessary. At a minimum, the TPA must be a U.S. citizen or be appropriately cleared by service/command authorities to the highest security level achieved by the KSV-21/STE.

c. The TPA is responsible for configuring the security straps in the STE to comply with any applicable local security policy. For example, in places where the speakerphone is not allowed, the TPA can disable the speakerphone in the STE through the menu option. Please refer to the STE User's Manual for a list of functions controlled by the TPA. The TPA also creates permanent associations between STE and KSV-21 cards. When necessary, the TPA can remove KSV-21 associations from the STE such as in the case of a lost user card.

d. The TPA must insert a designated TPA card into the STE to modify any security settings or perform card association with a STE. The first KSV-21 card inserted into a zeroized or factory configured STE is automatically given the option to register its serial number as the TPA card. A KSV-21 card can be the TPA card for a single STE or multiple STEs. That same TPA card can also be a user card for the same STE.

e. When the STE is zeroized, which can be accomplished by anyone via the STE menu, all its settings revert to defaults and any custom settings will have to be restored by the TPA. To prevent an inadvertent security violation, and when "Secure Only" is chosen as the standard operating mode for the STE, this setting and the audit information cannot be changed or deleted by zeroizing the STE, they can only be changed or deleted with a valid TPA card inserted.

f. The STE supports a TPA Transfer Function so that a new TPA card can be established based on a TPA password or pass phrase without the original TPA card, which may have been lost or damaged. However, there can be only one TPA card for a STE at any given time.

g. Each STE is shipped with two holographic tamper seals. When receiving STE shipments (regardless of whether the shipment came from a trusted or untrusted (improperly shipped) shipping channel or service), the TPA must examine the tamper seals for damage, verify that a TPA is not already established (some STEs may be shipped from previous sites) and review the audit log for previous serial numbers from a pre-existing TPA. Local policy may require that the TPA re-inspect the tamper seals on the STE for damage or breakage on a regular basis.

NOTES: 1. New units come zeroized and will have no TPA established.

2. TPAs are required to inspect tamper seals on STE units semi-annually. It is recommended to conduct these inspections in conjunction with FC inventories.

h. The password or pass phrase must be handled and stored appropriately in a secure container or filing cabinet.

i. Maintain all required logs, records, and files in accordance with paragraph 24 of this Annex.

j. **Software Upgrades:** Both the STE and KSV-21 card are software upgradeable in the field via the RS-232 data port of the STE. The signed software packages and the tools to do this are unclassified and can be saved to an unclassified computer. The KSV-21 card can only be upgraded through the STE cryptographic card interface and only if the KSV-21 card is associated with the STE.

k. The use of a computer to upgrade the STE and the KSV-21 does not change the computer's classification. The unclassified computer does not become classified because it was connected to the STE with a KSV-21 cryptographic card inserted. The STE disables all non-essential functions and disconnects itself from the telephone network during the upgrade process. In addition, the cryptographic keys cannot be exported outside the KSV-21 card while the STE or the card is being upgraded. In short, there is no classified information transferred to the computer during the software upgrade process for the STE and the KSV-21 card.

l. The following procedures are used to perform the upgrade. The software upgrade must first be downloaded from the L3 website to a file. Information and access to the site are available to the TPA once he/she registers as the TPA as specified in paragraph 6.a above. During the upgrade procedure, and if there is a software upgrade for the KSV-21 card, you will be prompted to upgrade the KSV-21 card software.

(1) Press “**Menu**”, terminal displays Terminal Management

(2) Press “**Select**”, terminal displays Network Setting

(3) Press “**Scroll**”, terminal displays Terminal Privileges, Association, and Software Update Management

(4) Press “**Modify**”, terminal displays Terminal Configuration Control

(5) Press “**Scroll**” 4 times, terminal displays the current software version

(6) Press “**Change**”, the terminal transitions through a Terminal Reset and will then display Update Software, Initiate Update from PC

(7) The software update is then executed by running the L3 Utility downloaded from the TPA web site.

NOTE: Information related to software upgrades or the latest releases can be found at: https://www.iad.gov/SecurePhone/index.cfm or http://www.iad.smil.mil.

5. **STE/KSV-21 User Responsibilities**:

a. A user who accepts the use of a KSV-21 card is solely responsible for safeguarding the card and cannot transfer the card without the knowledge of the Communications Security (COMSEC) 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. Unless prohibited by local security policy, the user card and/or carry card can be transported without written courier authorization.

b. An authorized person must supervise access by a person not having an appropriate clearance to a STE with a KSV-21 inserted.

NOTE: Additional information, including a listing of cards used by countries other than the U.S. can be found in NSA's DOC 007-07 located at: www.iad.smil.mil under the IA Library - doctrine tab.

c. A user must protect a KSV-21 card by either keeping it in the user's personal possession or storing it in a manner that will minimize the possibility of loss, unauthorized use, substitution, tampering, or breakage. In general, a user can send the KSV-21 card through X-ray machines or other security devices commonly used at the airports without harmful effect to the card.

d. Designated STE MC User will act in the capacity of the TPA for those commands he/she supports with STE keying material. Therefore, TPA responsibilities as specified in paragraph 4 apply.

6. **Keying Information**:

a. **KSV-21**: The KSV-21 fill card can be programmed with multiple Secure Data Network System (SDNS) keying universals and STE keying editions at the Electronic Key Management System Central Facility (EKMS CF).

b. Fill cards programmed with seed keys will have up to a five-year shelf life from the programming date. Usually the STE key edition and the SDNS key universal expiration dates determine the shelf life duration for a fill card. Seed keys must be converted to operational keys after the fill card is associated with the STE.

c. Fill cards programmed with operational keys will have a one-year shelf life from the programming date and can be used any time prior to its expiration. Operational keys can be used immediately to protect information traffic after the fill card has been associated with the STE.

d. Customer requirements to have KSV-21 cards reprogrammed (loaded with new keying material) must ensure the STE Key Order Request Form and SF-153, which is required to transfer the cards to EKMS account 880111, are included in the box with the cards that are being shipped to the EKMS CF. DO NOT FAX the key order to the EKMS CF. This could result in duplicate key orders being processed or the key order being returned.

e. The sending of KSV-21 cards back to the EKMS CF for hold and/or future storage is strictly prohibited. The EKMS CF cannot support this type of request/function. Only KSV-21 cards that arrive with a key order and proper SF-153 transfer report will be processed. Card shipments that are not accompanied by a STE Key Order Request Form and SF-153 will be returned to the sending EKMS account.

7. **Procedures for Establishing a TPA Card**: The first KSV-21 card inserted into a STE will become the TPA card. Prior to inserting, ensure that the STE is zeroized (in factory default state).

a. Insert a non-associated KSV-21 crypto card into the zeroized (e.g.; factory default state) STE

b. The terminal will read ***"Processing Crypto Card – please stand by"*** followed by ***"TPA Establishment XXXYYY as TPA"***

c. Press "**Select**", to confirm assignment of this card as the TPA.

d. The terminal will then display ***"Validating TPA Crypto Card – please stand by"***

e. The terminal will then display ***" TPA Establishment Successful – inserted card is TPA card"***

NOTE: The TPA Establishment does not affect the CIKS on the Crypto card. The card must be controlled under the same constraints as it was prior to the TPA establishment.

8. **Procedure for Creating a CIK Association with a STE**:

a. Press "**Menu**", terminal will display ***Terminal Management***

b. Press "**Select**", terminal will display ***Network Settings***

c. Press "**Scroll**", terminal will display ***Terminal Privileges, Association, and Software update management***

d. Press "**Modify**", terminal will display ***Terminal Configuration***

e. Press "**Scroll**" 3 times, terminal will display ***Create a new Association***

f. Press "**Create**", terminal will display ***Create Association - Insert User Card and Select Type***

g. Press "**Full CIK**", terminal will display ***Create Association Complete - Reinsert TPA Card or Done***

h. Press "**Done**", and the terminal will return to the Terminal Privileges, Association, and Software Update Management screen

> **NOTE: If the STE already has a TPA established, the TPA card will be required to complete the New Card Association: the STE will prompt the user to insert the TPA card before completing the association process.**

9. <u>**Conversions and Rekeying Numbers**</u>: Seed key conversion and rekey require two separate calls to the EKMS CF to allow for backwards compatibility.

a. For STE rekey the following worldwide rekey number are provided:

(1)	Commercial	410-526-3470
(2)	Toll Free	800-633-3971
(3)	DSN	312-238-4470

b. Problems connecting to the above listed numbers can be referred to the EKMS CF Technical Assistance Center (TAC) at the numbers listed below:

(1)	Commercial	410-526-3208
(2)	Toll Free	800-635-5689
(3)	DSN	238-4600 or 550-7884
(4)	United Kingdom	0800-96-8660
(5)	Germany	0800-827-8340
(6)	Italy	800-871936
(7)	Japan	00531-11-4208
(8)	Korea	00798-11-355-8256

NOTE: Electronic seed key conversion and rekey for SDNS key will require the STE to be connected to the ISDN. When FNBDT protocol becomes available, SDNS keying material can be converted or rekeyed independently of the telephone network connection.

10. **STE Rekey Procedures**: To perform a conversion/rekey you must first program the associated telephone numbers into the STE unit. Telephone numbers can be found in paragraph 9 (above).

a. Programming the rekey numbers into the STE unit:

(1) Press **"Menu"**, terminal displays ***Terminal Management***

(2) Press **"Scroll"**, terminal displays ***Crypto Card Management***

(3) Press **"Select"**, terminal displays ***Card Management Privileges***

(4) Select **"User"**, terminal displays ***Rekey Function***

(5) Press **"Select"**, terminal displays ***Update Rekey Phone Number/Perform Rekey***

(6) ***Select "Update", terminal displays Update Stored Phone Number***

(7) Select **"STU-III"**

(8) Enter rekey phone number and press **"Store"**

(9) Repeat procedures for additional numbers

11. **Performing a STE Rekey**: Ensure the action in paragraph 10.a. (above) is completed prior to attempting the STE Rekey procedure.

a. Press **"Menu"**, terminal displays ***Terminal Management***

b. Press **"Scroll"**, terminal displays ***Crypto Card Management***

c. Press **"Select"**, terminal displays ***Card Management Privileges***

d. Select **"User"**, terminal displays ***Rekey Function***

e. Press “**Select**”, terminal displays ***Update Rekey Phone Number/Perform Rekey***

f. Select “**Rekey**”, terminal displays ***Perform Rekey***

g. Select between “**STU-III**” and “**SDNS**”

h. Press “**GO**”

i. Terminal will prompt you to press “**Continue**” upon completion of rekey.

All operational keys have a one-year cryptoperiod. At the end of the cryptoperiod, the user must call the EKMS CF for new operational keys. Rekey calls may be placed at any time prior to the expiration date. Once the rekey calls are complete, the user must verify that the dates have changed and have been extended for another year. If it is not possible to call the EKMS CF, new operational keys must be manually loaded in the KSV-21 card.

12. **STE Accountability, Classification, and Handling**:

a. The STE is unclassified equipment and does NOT require accountability within the COMSEC Material Control System (CMCS). COMSEC Custodians should not take possession of the STE unless directed by their agency or organization. The STE is a high dollar value sensitive, pilferable item; therefore, standard department and agency logistics, property accounting, and security controls must be strictly adhered to.

b. The STE must be protected in a manner sufficient to prevent loss and tampering. A STE with a cryptographic card inserted may not be left unattended to prevent possible unauthorized use. However, the STE may be left unattended when a cryptographic card is not inserted.

13. **Residence Installation**: A STE terminal may be installed in the residence of a U.S. Government, contractor officials or in residences of state, territorial, and local government officials when they are authorized to have such secure telephone devices, under the directions or sponsorship of an authorized Government official. Only the person for whom it was installed shall use the STE. All of the security requirements should be observed for preventing unauthorized access to the keyed terminal and to classified and sensitive unclassified U.S. Government information. The KSV-21 card should be removed from

the terminal following each use and kept in the personal possession of the user, or stored in a security container approved for the classification level of the terminal's key. When the terminal is used in data mode, classified information that is viewed on the screen should be removed as soon as possible, and should not be printed out unless there is appropriate classified storage. The following installation types are approved:

a. **Typical Installations**: Normally, the key authorized for use in residential installations shall be limited to the UNCLASIFIED level. The secure telephone device shall be keyed such that "RESIDENCE" will appear in the display window of the distant device. The display merely shows the approved security level of the environment in which the secure telephone device is located. However, if classified discussions are absolutely necessary and authentication of the remote part is possible (e.g., via positive voice recognition), then only the party in the secure area may pass classified information. In the non-secure area (e.g., the residence), the party is restricted to merely hearing classified information. Unless appropriate storage is available, any notes taken by the residential user during such conversations must be limited to UNCLASSIFIED information. Likewise, all comments made must be limited to the UNCLASSIFIED level because the residential environment is not secure. The non-residential user must verify the identity of the residential user and observe clearance level and need-to-know restrictions before transmitting any classified information.

NOTE: When ordering key for a residential installation, the Key Ordering Authority must be notified of its intended use so that "RESIDENCE" can be included in the information to be displayed.

b. **Installations Permitted with Approval of Local Security Official**: Information shown in the display window of a secure telephone device must properly reflect the physical location (e.g., RESIDENCE) of the device. It does not necessarily reflect the level of classified information that may be discussed. If the residence has been approved as a secure area (e.g., a cleared facility), the secure telephone device may contain key indicating SECRET or TOP SECRET, at the discretion of the local security official who must approve the physical security conditions of the environment. If an area of residence has been officially upgraded to a Sensitive Compartmented Information Facility (SCIF), then TS/SI might be appropriate for the key. Please note that by definition, "A SCIF is an accredited area, room, group of rooms, buildings, or installation where SCI may be stored, used, discussed, and/or electronically processed". The local security official, aided by applicable department or agency guidelines, must approve the security level of the key as well as the environment in which it is use.

c. **Additional Considerations (General)**: Since secure telephone devices may be operated in non-secure environments, most of which are not consistent with classified use of the phone, it is necessary to pay special attention to how and where such telephones are used. To minimize the necessity for applying additional security restrictions, local security officials and users should consider the following recommendations to reduce the level of risk:

NOTE: Local security officials should discuss threats with users and have users acknowledge, in writing, that they understand the risks of using these devices and are willing to abide by the restrictions imposed by applicable national, departmental, or local policy.

(1) When talking at a classified or sensitive level, the user must be aware of the surrounding environmental conditions, including the proximity of any uncleared or unauthorized individuals.

(2) The local security officials should implement a common-sense approach to address acoustic security concerns. Introduction of the secure telephone device into an area where classified or sensitive unclassified operations are conducted should not change the normal security requirements for the area. Ideally, all persons assigned to an area where classified work is carried out should have the same clearance. Where this is not possible or practical, local procedures should be implemented to prevent uncleared persons assigned to, or temporarily in, the area from overhearing classified face-to-face or telephone conversations.

(3) The user must always verify the telephone is in the secure mode prior to using it for classified or sensitive conversations.

(4) Before beginning a secure conversation, check the display to verify appropriate security level has been

achieved. Users should not normally exceed the classification level indicated on the display. Because of interoperability among telephones of different classification levels, the display may indicate a security level less than the actual classification of one telephone's key (e.g., when a TOP SECRET telephone calls a SECRET telephone, "SECRET" is displayed on both devices as the authorized level for the call). Also, the user must be cognizant of special conditions associated with the phone at the distant location (e.g., RESIDENCE, MOBILE etc.). Therefore, users must observe the display with each call and limit the level of information accordingly.

(5) Paragraph 13 states that the secure telephone "when installed in a private residence, shall only be used by the person for whom it was installed". While any secure telephone device may be used on an occasional basis by family members in a residence or by uncleared personnel in an office, such individuals must not have access to the security-enabling component (KSV-21 card). Uncleared/"unauthorized" persons are restricted to only using the telephone in its commercial non-secure mode. Department or agency regulations may prohibit all non-official use of government owned telephones. If the security-enabling component is compromised, or an uncleared/unauthorized person gains access to it, this must be reported as a COMSEC incident.

14. **STE Data Port**: The STE offers similar Secure Access Control System (SACS) features to those found in the previously used STU-IIIs; they can be applied in both voice and data during secure call setup. For unattended classified data applications, SACS or an equivalent security system is required. SACS is made up of three components, an Access Control List (ACL), a Minimum Security Level (MINSL), and a Maximum Security Level (MAXSL). Do not use any secure telephone device in the data mode while it is unattended in a non-secure environment.

A double-shielded cable (for example, INMAC 0655-1) is required for data applications requiring TEMPEST compliance.
If it becomes necessary to use the secure data mode of the terminal (e.g., with a fax machine or computer) the requirements set forth in the Security Doctrine for the Enhanced Cryptographic Card (ECC) and STE must be adhered to.

15. **Destruction**: STE equipment that is unserviceable and out of warranty will be serviced and disposed of in accordance with local command policy regarding excess property. Service beyond the warranty originally purchased with the STE is the sole

responsibility of the purchasing command. SSC Atlantic performs screening and repair of defective STE terminals when a device can be repaired. For assistance with STEs contact the Global Distance Support Center at 1-877-418-6824. Defective terminals can be shipped to the address in the note below this paragraph. In emergency conditions, to prevent the STE or KSV-21 from being captured by terrorists or a hostile enemy force, both the STE and KSV-21 must be physically destroyed if they cannot be safely evacuated. The KSV-21, if at all possible should be destroyed before the STE.

NOTE: SSC ATLANTIC CODE 55360
ST. JULIENS CREEK ANNEX
BUILDING 12 WATER ST.
PORTSMOUTH, VA 23702

ATTN: KEN ZINSMASTER
TELE: 757-541-5015

16. **<u>KSV-21 Accountability, Classification, and Handling</u>**:

a. The KSV-21 card contains cryptography and it is assigned Accounting Legend (AL) Code 1 (AL Code 1). This means that the KSV-21 card must be accounted for within the COMSEC Material Control System (CMCS) by its unique serial number, not the keying material identification number on the tags, until the card is physically destroyed. The EKMS Manager must inventory the package upon receipt, sign the accompanying SF-153 if a physical shipment, enter the material into accountability, and return the SF-153 to the CF and Central Office of Records (COR) if appropriate. Electronic shipments can be receipted for electronically. In light of the recent terrorist activities and increased security precautions that delay first class mail, delivery of SF-153s via fax to the EKMS CF is authorized. The following SF-153 faxing information applies:

Key Orders (e.g., STE, SDNS, etc.) and registration forms (e.g., DAO Registration Requests, User Representative Registration Requests, etc.) can be faxed to the following:

COMM	(410) 526-3172	or	DSN	238-4127
	(410) 526-3454	or	DSN	238-4454

All signed SF-153 receipts for CA 880103/880104/880111/880335 can be faxed to the following:

COMM (410) 517-3321 or DSN 238-4321

NOTE: Please do not fax EKMS account inventories due to the large amounts of paperwork associated with inventories. Continue to use U.S. registered mail or alternate methods for this purpose.

b. The KSV-21 card can only be procured, installed, and operated by U.S. Government departments or agencies and their contractors who have an EKMS account. A KSV-21 card programmed with keying material can only be issued to a properly cleared user who possesses a clearance level equal to or greater than the keying material on the card.

c. A KSV-21 card **may be a Fill, Seed, User, Carry, TPA, or Unkeyed (zeroized) card**. With the exception of the fill card, all cards are UNCLASSIFIED but must be protected by being either in the user's personal possession or stored in a manner that will minimize the possibility of loss, unauthorized use, substitution, tampering, or breakage.

(1) A fill card is a keyed KSV-21 card that has not been associated with the STE (may take up to 3 weeks for delivery). A fill card may be programmed with seed, test, or operational keying material and is accountable to the Central Office of Record (COR). A TPA (EKMS Manager) can perform the association process for the user or issue the card on hand receipt to the intended user for the purpose of associating the card with the STE.

(2) A fill card programmed with seed or test keying material is UNCLASSIFIED and can be handled and stored in a manner that will reasonably preclude any chance of theft, sabotage, tampering, or use by unauthorized personnel.

(3) A fill card programmed with operational key material must be handled and stored in a manner consistent with the classification of the key material. This type of fill card must be stored in a safe or container approved for storing cryptographic keying material. Two-Person Integrity (TPI) handling and storage are **NOT** required even fill cards programmed with compartmented TOP SECRET operational keying material because the anti-tamper features in the card prevent keys from being read or duplicated.

(4) The EKMS CF normally seals a fill card in a protective plastic package. The protective packaging of the

fill card must not be opened until the card is ready to be associated with the STE. The protective packaging must be properly disposed of in accordance with local security policy.

(5) A fill card is packaged with two associated key tags. Each key tag displays a short title, a key edition or an SDNS key universal, and a unique keying material registration number. It is possible that a card may be programmed with more than one SDNS universal (e.g., U.S. and UK universals). The information on the key tags is used to verify keying material on the fill cards once the STE association process has been performed. The key tags are then kept locally for reference and can also be used to construct an Access Control List (ACL) if one is needed.

(6) A fill card must not be used solely as a TPA card and/or carry card. A fill card may initially be used to create a TPA card but must be immediately associated to at least one STE as a user card.

(7) The preferred card is the seed card. Seed Cards have limited command information based on the Key Order Request submitted, is UNCLASSIFIED and can be handled and stored as specified in subparagraph (c) above. Seed Cards must go through the rekey process to have the SDNS key put on the card from the CF via the rekey. Once completed, the seed card now becomes a User Card.

17. **Issuing KSV-21 Cards**: KSV-21 User, Carry or TPA cards can be issued one of the following ways:

a. SF-153 Transfer (Local Custody)

(1) Locally generated Local Custody form. Locally generated forms are **only authorized at the MC User level.** When issued at the Manager level, all issues will be conducted using LCMS are outlined in Article 715. Example form is provided as Figure AD-1.

b. **Inventory Requirements**: Fill cards must be 100 percent physically inventoried and sighted. The EKMS Manager and an EKMS witness must perform the inventory for fill cards being held in the account.

(1) Each fill card and its associated key tags are packaged in a sealed transparent protective container at the EKMS CF. The container must not be opened for audit and

inventory purposes. Inventories for STE MC Users will be generated in accordance with local command instructions. All required information must be present on the inventory that is consistent with the tracking of AL Code 1 COMSEC material (see Article 230 of this manual) STE MC Users will inventory those fill cards issued to them, both the STE MC User and an appropriately cleared EKMS witness will sign the inventory report and return the results of the inventory to the EKMS manager.

(2) Cards that are issued to users do not require an EKMS witness for an audit. A hand receipt will be issued for cards that cannot be physically sighted.

(3) Cards issued to LEs which operate in a watch-type environment will be reflected on and accounted for via a watch-to-watch inventory.

c. **Destruction**: KSV-21 cards that become unserviceable and are no longer under warranty may be shipped to the following address for disposal. An SF-153 Transfer Report must accompany the card.

Director, National Security Agency
Attn: S714 (Account 889999)
Fort George Meade, MD 20755

In emergency conditions, to prevent the KSV-21 or STE from being captured by terrorists or a hostile enemy force, the KSV-21 and the STE must be physically destroyed if they cannot be safely evacuated. If at all possible, the KSV-21 should be destroyed before the STE.

d. **Key Conversion Notices(KCN)**: Seed key destructions are normally registered with the EKMS CF by the seed key conversion call. This call to the EKMS CF converts the keying material for operational use, provides the terminal with the Compromise Information Message (CIM) and Compromise Key List (CKL), and registers the destruction of the keying material with the EKMS CF database.

The KCN is not generated by the EKMS Manager or MC User, but by the EKMS CF. The EKMS CF distributes a KCN to each account. This notice will be forwarded to the account only after rekey calls to the EKMS CF have been made. All seed key converted by that account (by phone call to the EKMS CF) will appear on the notice. If Type 1 Operational Key is held by the account, the

KCN will also list all operational key for which a rekey call was made prior to the EKMS CF receiving an SF-153 Destruction Report from that account. A brief description of the KCN and required actions follow:

(1) Required Action. The EKMS Manager must verify the information provided on the KCN. Specifically, for each item of seed key listed, the EKMS Manager must:

(a) Enter the date of the KCN in the A/I Summary to document seed keying material destruction.

(b) Verify that the terminal serial number listed is the serial number of the terminal in which the key was loaded.

(c) Ensure that all keying material listed was, in fact, held and loaded/destroyed by the account as indicated on the report. Accounts must also prepare a "Filled in End Equipment" destruction for that key and send the report to the COR.

(2) **Reporting Discrepancies.** Whenever keying material listed on a KCN is still maintained by the account (that is, remains unused), it must be reported as a COMSEC Material Incident in accordance with paragraph 25 of this annex.

(3) See Article 792 and EKMS-702.06 for additional information regarding the destruction and related reporting for modern key.

18. Procedures for Zeroizing a key from the KSV-21 Card

(TPA must have Card Privileges enabled)

a. Press "**Menu**", terminal will display Terminal Management

b. Press "**Scroll**", terminal will display Crypto Card Management

c. Press "**Select**", terminal will display Card Management Privileges

d. Press "**User**", terminal reads View Card Key Data

e. Press "**Scroll**", terminal reads Zeroize key

f. Press “**Select**”, terminal reads Zeroize specific key and gives KMID #

g. Press “**Select**” or “**Next**”

h. Confirm your choice

NOTE: Remember, there are 2 keys on the KSV-21!

19. **Procedures for Removing Terminal/Card Associations**

(TPA must have Card Privileges enabled)

a. Press “**Menu**”, terminal will display Terminal Management

b. Press “**Scroll**”, terminal will display Crypto Card Management

c. Press “**Select**”, terminal will display Card Management Privileges

d. Press “**User**”, terminal reads View Card Key Data

e. Press “**Scroll**” twice, terminal displays Remove Terminal/Card Association

f. Confirm your choice

20. **Transporting STEs**:

The STE may be delivered by any commercial carrier providing the carrier possesses a means of tracking individual packages within its system. Tracking should be to the extent that should a package become lost, the carrier can, within 24 hours following notification, provide information regarding the last known location of the package(s). STEs are not CCI equipment or accountable in the CMCS.

21. **Transporting KSV-21s**:

a. Fill cards are normally packaged in sealed transparent protective technology plastic and must be handled and shipped similarly to cryptographic keying material of the same classification. For more specific guidance, refer to Article 530 of this manual.

b. With the exception of a fill card, all cards may be delivered by U.S. Registered Mail, courier, in person, or a commercial carrier that provides continuous tracking provided that associated cards are not packaged together.

c. The KSV-21 should not be packaged in the same container with their associated STE for shipping. When using commercial carriers, the KSV-21 should be shipped via separate carrier or channel from that of an associated STE to minimize the risk. If the same commercial carrier or channel is used, the KSV-21 must be shipped on a different day from that of their associated STE.

d. The user card and its associated carry card should not be packaged in the same container. When using commercial carriers, the user card should be shipped via separate carrier or channel from that of the carry card. If the same carrier is used for shipment, the user card must be shipped on a different day from that of the associated carry card.

e. If the STE and its associated user card or if the user card and its associated carry card cannot be separated for shipping, they will be packaged and transported as classified material in a manner consistent with the classification level of keying material on the card.

f. Prior to shipping the card(s) back to the EKMS CF or the card manufacturer, the KSV-21 card(s) must be zeroized or all card and terminal associations removed. Be aware that the key zeroization is available only when the TPA has enabled "card privileges" and that each key set or type must be independently zeroized until the card is completely empty. When an EKMS account transfers/ships materials to the EKMS CF, regardless of shipping method (e.g., FEDEX, Airborne Express, U.S. Registered or Express Mail), the sending account should identify the account number of the account the material is being transferred to (e.g., CA880103/880104/880111 or 880335) on the outer shipping label of the package. Whenever possible, include a point of contact name with the EKMS account number.

(1) A KSV-21 fill card can be zeroized via the STE. **An EKMS witness is required when zeroizing a fill card with operational key and an SF-153 Destruction Report must be generated.** A preferred method that does not require an EKMS witness is to associate the fill card with the STE first and then either convert or rekey electronically to the EKMS CF, after which the card can be zeroized via the STE. Procedures

for key zeroization and conversion via a rekey call are located in paragraph 18 and paragraph 11 respectively.

(2) If a malfunction prevents a fill card from being zeroized via the STE then it must be shipped to the EKMS CF as a classified item equal to the security level of the cryptographic keys programmed in the card. The procedures for shipping classified items can be found in Chapter 5 of this manual. A fill card that failed zeroization **shall not** be shipped to the card vendor for service.

(3) If a malfunction prevents a user card from being zeroized via the STE then its association must be removed from all associated STEs. A user card has the option to remove its own association at the associated STE if the TPA has enabled "card privileges". However, if a malfunction (or if the user card is lost) prevents the removal of its association with the STE then the TPA card can be used to delete the serial number of the card from the associated list.

22. Exceptions – Transportation Within U.S., Its Territories, and Possessions

a. Authorized users may transport cards personally.

b. U.S. Government department, agency, or contractor couriers may be authorized to transport cards.

c. U.S. Registered Mail or any commercial carrier that can satisfy the following requirements may transport cards:

d. Be a firm incorporated in the U.S. and provide door-to-door service;

e. Guarantee delivery within a reasonable number of days based on the distance to be traveled;

f. Have a means of tracking individual packages within its system to the extent that, should a package become lost, the carrier can, within 24 hours following notification, provide information regarding the package's last known location;

g. Guarantee the integrity of the shipping vehicle's contents at all times; and

h. Guarantee that the package will be afforded a reasonable degree of protection against theft (e.g., use of a security cage, video surveillance, etc.) should it become necessary for the carrier to make a prolonged stop at a carrier terminal.

23. **Exceptions - Transportation Outside U.S., Its Territories, and Possessions**

a. Authorized users may transport cards personally.

b. U.S. Government department, service or agency couriers may be authorized to transport KSV-21 cards.

c. U.S. Postal Service (USPS) Registered Mail may be used to ship KSV-21 cards providing the material does not, at any time, pass out of U.S. control, pass through any foreign postal system, or become subjected to any foreign postal inspection. USPS Registered Mail may be used to ship KSV-21 cards to/from locations overseas, but only if the location is serviced by a Fleet Post Office (FPO) or Army/Air Force Post Office (APO) that is authorized to process USPS Registered Mail.

d. U.S. military or military-contract air service carriers (e.g., AMC, Logair, and Quicktrans) may be used to ship KSV-21 cards provided there is a continuous chain of accountability for the material while it is in transit. To the maximum extent possible, material shipped to/from locations outside the U.S., its territories and possessions should remain under continuous U.S. control. Although some limited handling of the material by foreign nationals may be unavoidable during aircraft loading and unloading operations, the material must be returned to U.S. control upon completion of these operations. Should a KSV-21 subsequently show evidence of unauthorized access or tampering, a COMSEC incident report shall be submitted to the DIRNSA//I31132// within 12 hours upon the discovery of the incident. See paragraph 25 for unauthorized access or tampering of the STE.

24. **Required Logs, Records and Files**

All applicable logs, records and files will be maintained in accordance with Chapter 7 of this manual.

25. **STE COMSEC Incidents/Practices Dangerous to Security (PDS):**

a. The following incidents will be reported to DIRNSA//I31132// in accordance with procedures outlined in

Chapter 9 of this manual.

(1) Failure of the COMSEC Custodian to notify EKMS CF that seed keying material listed on the Key Conversion Notice (KCN) still exists in his/her account (never used).

(2) Mismatch of keying material on the cards and key tags (keying information can be verified after STE association).

(3) Whenever the user identification or authentication information displayed during a secure call is not representative of the distant terminal. Authentication information includes:

(4) Authorization for access to sensitive compartmented information (SCI) when common to both terminals.

(5) Identification of the using organization (e.g.; US Navy, US Army)

(6) Foreign access to a keyed terminal, when approved (e.g.; CANADA) identifies terminals supporting Canadian operations, (US/CAN) identifies terminals supporting US/CAN operations.

(7) Any instance in which the display indicates that the distant terminal contains compromised key.

(8) Known or suspected tampering of a KSV-21 card.

(9) Loss of a fill card.

(10) Loss of a card when the card can be identified with a particular secure voice or data terminal and it was not disassociated from its terminal.

(11) Loss of a user card **with** its associated carry card.

(12) Loss of a user card **with** its associated STE.

b. Reportable Practice Dangerous to Security (PDS)

(1) Loss of a User Card. Users are required to notify the TPA when a user card or carry card is lost so that

its association with the STE can be removed at the earliest opportunity to prevent unauthorized access to the STE. TPAs at the LE (Issuing) level must notify their respective EKMS Manager who will report the matter as a reportable PDS to the agencies reflected in Article 1010.c using the subject "REPORTABLE PDS LOSS OF A KSV-21 CARD". At a minimum the message will include four paragraphs as illustrated:

(1) EKMS ID Number and HCI
(2) List the Unit POC
(3) Provide a brief description of the circumstances surrounding the loss.
(4) List corrective actions to prevent and/or minimize future occurrences of this nature.

(2) Loss of a TPA card. Loss of a TPA card may impact local information security because a TPA card can be used to change the security settings of all the STEs under its control. Each location that uses a TPA card to enforce local security straps in the STE must re-establish a new TPA card for the affected STEs at the earliest possible opportunity. The STE supports the TPA transfer function so that a new TPA can be established base on a TPA password or pass phrase without the original card that is lost or damaged. However, there can be only one TPA card for a STE at any given time.

c. The following are locally reportable Practice Dangerous to Security:

NOTE: Commands will report these PDSs as soon as possible after their occurrence or upon their discovery to the appropriate agencies.

(1) Discovery of a tampered or unauthorized modification/repair of a STE. The STE is not a COMSEC device and this **IS NOT** considered a COMSEC incident. However, the integrity of the STE must be verified prior to installation for operational use. Users must contact their EKMS Managers for specific guidance. EKMS Managers can contact the STE program office at NSA for further assistance upon discovery of unauthorized repair or modification of a STE.

26. **Maintenance**: Both the STE and the KSV-21 shall be serviced by the original vendor of authorized personnel. Any attempt to open the KSV-21 other that by the original manufacturer is prohibited. Refer to the STE Operations Manual for points of contact and telephone numbers.

TAB 1 TO ANNEX AD TO EKMS 1B

IRIDIUM SECURE MODULE (ISM)

1. **Introduction to ISM**: The ISM is designed for use with the Motorola 9505 (Laguna) Iridium satellite telephone. The ISM/Iridium satellite telephone is a lightweight, handheld Future Narrow Band Digital Terminal (FNBDT) compatible device designed to provide users worldwide secure voice connectivity in mobile environments as well as secure voice connectivity to desktop STEs. The user activates the secure voice capability of the ISM by entering a user assigned personal identification number (PIN).

a. Appropriately keyed ISMs are approved to protect information of all classifications and categories.

b. The ISM is a Type 1 only piece of equipment.

2. **Control Requirements**:

The ISM is a Controlled Cryptographic Item (CCI) and will be handled as such in accordance with Article 535 of this manual. When the secure capability of the ISM has been activated, by entering the user ISM PIN code, the device must be protected to the classification level of the key it contains.

3. **Accounting Requirements**:

The ISM is accountable by its serial number. The ISM is Accounting Legend (AL) Code 1, therefore is accountable within the COMSEC Material Control System (CMCS) and will appear on COR-generated inventories.

NOTE: The Short Title for the Iridium is FNBA20 and the. ISM serial number can be found on a label placed on the unit.

4. **Storage and Handling**:

a. So as not to overly inhibit its use, an ISM that has been loaded with key may be handled the same as an ISM without key, provided the PIN code remains separate from the device.

b. The ISM user must maintain continuous physical control of the device or keep it stored in a manner that will minimize the possibility of loss, theft, unauthorized use, or tampering.

5. **Transportation**:

a. ISM devices, with or without key (zeroized), shall be shipped in accordance with the guidance contained in Article 535 of this manual.

b. A U.S. user may carry an ISM as an item of personal property to locations outside the United States, its territories and possessions, provided its use is restricted to official purposes only. To reduce the level of risk, ISM users should consider the following recommendations:

c. When talking at a classified/sensitive level or entering a PIN code, be aware of environmental conditions, including the proximity of uncleared individuals. Although the ISM can secure a telephone conversation, it cannot secure the surroundings.

d. Keep the ISM PIN code separate from the ISM.

6. **Keying Information**: The ISM Key Order Request may be obtained from the EKMS CF by calling 1-800-635-5689 and following the directions for Fax Back services. The Command Authority (CA), or User Representative (UR) must complete the form and then sent it to the CF. Each ISM is filled with operational key via a DTD. Procedures for obtaining electronic key from the CF, transferring the key to the DTD and then filling the ISM are specified below:

7. **Procedures for Obtaining and Downloading Electronic Key**:

a. **FIREFLY Credentials**: Prior to receiving electronic key from the CF, you must ensure that the KP FIREFLY vector set is up to date (not expired) and at the KP effective FIREFLY credentials are posted to account 880091.

b. Place your Key Order Request to the CF.

c. **Downloading Key from the X.400 Server**:

(1) Logon to LCMS and the KP.

(2) Ensure the A/B/C/D switch is set to position B, Central Facility (CF).

(3) Double click the X.400 icon and select **Connect.**

(4) Dial the CF, wait for the secure data light on the STE and then click OK. The system will establish a connection with the CF and check for incoming mail. If no mail is available, your key order has not been processed. Wait 24 hours and try again.

(5) If mail is available, ensure **Receive** is selected, highlight the message(s) to download, and select **Process.**

(6) After all mail is processed, disconnect from the CF and return to the LCMS desktop.

(7) **Unwrap** the received transactions. You will have a bulk encryption transaction (BET) on the desktop.

(8) Process the BET by selecting **Accounting, Reconciliation, Reconcile Electronic Package.** Select the Package(s) to process, drop to the lower window and click **Process Transaction.**

(9) After processing, a receipt transaction is created on the desktop. This receipt transaction <u>**must be wrapped**</u> for account 880091 <u>**and transmitted**</u> using the X.400 tool. **Do not** report receipt to NCMS.

8. <u>**Loading Key into the DTD**</u>:

a. Logon to LCMS and the KP.

b. Ensure the local element (DTD) is set for unencrypted delivery via DTD.

c. Attach DTD to KP red fill port.

d. Power on DTD and select the **D101 Protocol** in the fill application.

e. In LCMS, select **Distribution, Manual, Electronic Key to Element.** Select the element for issue and click **Select.**

f. Select the key(s) to be loaded into the DTD and drop to the lower window. Click **Update Segments.**

g. Enter a distribution file name (this can be any DOS formatted (8X3) file name) and click **Distribute Keys**.

h. On the DTD, select **Receive** and start the receive process.

i. Click **OK** in LCMS to initiate issue.

j. If key is not registered, the DTD will prompt for a text ID. Enter desired text (e.g., Iridium etc.) or press **Enter** to bypass.

k. An issue report (hand receipt) will be created on the desktop.

NOTE: A hand receipt must be provided as a basis of receipt, inventory and reconciliation for keys issued from the LMD/KP to any FD (see Article 769.h.)

9. **Initial Keying and Rekeying Information**:

a. When the ISM does not contain key, the Type 1 Disabling Software (T1DSW) PIN code must be entered before key can be loaded. Keying material is loaded into the ISM via a DTD.

b. Since the ISM does not have over-the-air electronic rekey capability, it must be rekeyed manually.

c. An ISM rekey is required whenever the key has expired (one-year cryptoperiod) or whenever otherwise directed by the CF. The ISM shall be rekeyed whenever the key in the device has been compromised. In addition, the ISM requires a rekey whenever the device has been zeroized (either accidentally or intentionally) or a new key of a different classification/category is needed for the unit.

10. **Automatic Disabling Feature**:

a. The ISM keying capability is protected with the 8 digit T1DSW PIN code. The ISM allows ten attempts to unlock the module and allow keying. If ten entries are exceeded, the ISM becomes disabled and will not allow key loading operations. The ISM must then be returned to the General Dynamics repair depot for re-enabling. Contact the General Dynamics Customer Care line at 877-449-0600. Once all your information is collected (including billing information, if applicable), a return authorization will be issued. The pre-addressed label will have the shipping address along with the EKMS account number in which to transfer the unit via SF-153. Ensure to annotate the SF-153 citing the authority for transfer as warranty repair/replacement or out of warranty repair/replacement.

b. The four-digit user PIN code allows secure use of the phone and is generated after keying material is loaded into the ISM. The user has 4 attempts to enter the PIN code correctly. If the PIN code is entered 4 times incorrectly, the keying material will be zeroized automatically. The keying material must then be reloaded into the device.

11. **Loading your ISM**: Follow the instructions on page 38 (Loading Your ISM with SDNS Type 1 Encryption Key from an AN/CYZ 10 Data Transfer Device (DTD)) of the Iridium Security Module User's Guide. Additional guidance is as follows:

a. The DTD must be set to the LMD protocol (press Utility, Setup, Protocol, LMD).

b. When transmitting key from the DTD, select **Fill not Issue**.

c. If the load is unsuccessful after two tries, use a different key.

IMPORTANT NOTICE: When loading Operational keying material in the ISM, the user EKMS Manager should record the Key Management Identification number (KMID) and the terminal serial number. In the event the terminal is compromised or lost, the KMID can be readily provided to the EKMS CF to be added to the Compromised Key List (CKL). Without the user generated PIN code, the terminal serial number and the KMID together are only UNCLASSIFIED//FOR OFFICIAL USE ONLY.

12. **Recording Loading/Destruction of ISM Key**:

a. Zeroize key from DTD.

b. In LCMS, select Accounting, Destruction, Record Filled in End Equipment.

c. Select keys for destruction and drop to lower window.

d. Click Record Fill Equip. Material will be marked as destroyed and will appear on the next consolidated destruction report.

13. **PIN Information**:

a. The ISM manufacturer shall assign a unique T1DSW PIN code to each ISM. The ISM shall be shipped separately from the T1DSW PIN code to the user's EKMS account as indicated on the key order request. This eight digit T1DSW PIN code enables the ISM to be keyed. The Motorola depot maintains a list of these PIN codes. Command Authorities or User Representatives can call the Motorola Depot for access to their T1DSW PIN codes if they are lost or destroyed.

b. After the ISM is keyed, a four-digit ISM PIN code enables the secure use of the phone. The ISM PIN code is generated by the user and shall be reported to the appropriate authority in order to enable the list generation described in paragraph 3.b.(5) below. Selection of ISM PIN codes shall follow good security practices. **Do not** use personal items such as birth dates, part of your SSN etc. when selecting PINs.

c. Both the PIN codes are unclassified as long as they are not directly associated with a specific ISM device. Neither the T1DSW PIN code nor the ISM PIN code shall be written on, or otherwise affixed to the ISM.

d. The ISM does not have an over-the-air electronic rekey function. It is, therefore, recommended that the user record and appropriately safeguard all PIN codes to prevent unnecessary physical rekeys.

e. Activities holding multiple ISM devices are authorized to generate a list of ISM PIN codes (T1DSW and user) which will be maintained by the CA, UR or EKMS Manager.

14. **Disposition**: Activities should contact the DIRNSA Asset Management Office (410-854-6154) before disposing of an ISM that is excess to the activity's needs.

If the ISM device becomes unserviceable and is out of warranty, it should be shipped to the DIRNSA Information Assurance secure Wired/Wireless Technologies Division:

Commercial:
NSA (CA880618)

Attn: Wired/Wireless Technologies
9800 Savage Rd., Suite 6733
Ft. Meade, MD 20755-6733

DCS:
880618-BA21
NSA/CSS DIR I221
FT MEADE MD

15. **Destruction**: User destruction of the ISM is not authorized without approval from DIRNSA. If an unserviceable ISM is still under warranty, instructions in the manufacturer's handbook should be followed. All excess or unserviceable ISMs should be zeroized prior to shipment for repair/replacement.

If the ISM cannot be zeroized, it shall be handled in a manner consistent with the classification level of the key it holds.

16. **COMSEC Incidents**: The following incidents will be reported to DIRNSA//I31132// within 12 hours following the discovery of the incident in accordance with Chapter 9 of this manual.

a. Evidence of possible tampering with, or unauthorized access to a keyed ISM.

b. Loss or theft of an ISM.

17. **Maintenance**:

a. **In-Warranty**: The ISM contains no user replaceable parts. The original vendor shall perform all maintenance actions. Users shall not attempt to open an ISM.

b. **Out-of-Warranty**: Activities should send a message to NCMS//N31// requesting disposition instructions. The message should include: short title and serial number(s) of the equipment.

[EKMS Account ID]

Date: 00/00/00
Page 1 of 1

STE/KSV-21 Holder Listing

Name: Smith, John S. Rank: LT Clearance: TS
Location: Admiral's Aide Phone: 999-999-9999 Office Code: N6

ITEM	KSV-21 S/N	ALC	QTY	TYPE CARD [1] [2] [3]	STE TERMINAL S/N [4]
1		1	1	1	STEA3000009018
2		1	1	2/3	STEA3000009018

Statement of Responsibility

The above KSV-21 listing corresponds to the KSV-21s that have been issued to you. Each KSV-21 is an unclassified, locally accountable Communications Security (COMSEC) item. You must institute local controls limiting access to the keyed Terminal and KSV-21 inserted to those persons who have appropriate Security Clearance and Need-To-Know. The terminal, when unkeyed and the 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 MC User may be reached by phone during normal working hours at (000)000-0000. After hours contact ___________ at (000)000-0000.

I, the person whose signature appears below, certify that I have in my possession and hold myself responsible for the STE materials 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.

FIGURE AD-1

ANNEX AE

MANAGEMENT OF MODERN KEY

1. **PURPOSE.** This annex is intended to provide guidance related to the acquisition, destruction, handling, management and use of asymmetric keying material used for Secure Data Network System (SDNS) and Secure Communication Interoperability Protocol (SCIP) products. SDNS and SCIP products include but are not limited to FIREFLY and Enhanced FIREFLY key.

Throughout this annex, the use of asymmetric, modern, SDNS or SCIP all refer to the same type of products. The use of symmetric or traditional pertains to traditional keying material. The use of COMSEC Account Manager herein is referring to the EKMS Manager or Alternates.

2. **MODERN AND TRADITIONAL KEYING MATERIAL DIFFERENCES.** Some unique differences exist between asymmetric (modern) and symmetric (traditional) keying material which managers should be aware of, including but not limited to:

a. Modern key must be ordered, it is not distributed automatically based on distribution profiles, supersession dates, reserve on board (ROB) levels or deployment messages used for traditional keying material.

b. For modern key, the role of a Controlling Authority does not exist. The responsibilities, while very similar in nature are performed by a Command Authority.

c. To acquire asymmetric keying material, the requestor must have User Privileges validated by the Command Authority, be registered at the Central Facility (CF) and have a Defense Organization Code (DAO) established or previously registered at the CF. Appointment as a COMSEC Account Manager or being reflected in the accounts Common Account Data (CAD) does not authorize such personnel to order modern key.

d. The CF Form 1206 is used to register, modify or delete User Representatives and must be completed and submitted to the unit’s Command Authority for validation and submission to the Central Facility via the interactive registration tool found at https://www.iad.gov/keysupport.

e. Unlike with traditional keying material, there are no per-se effective and supersession dates for modern keying material. Modern keying material has an expiration date and is effective for one-year from the date it was produced or converted if the key is seed key converted through the rekey process not one-year from the date issued, loaded or used at the unit level.

f. Seed keying material supersedes when the associated universal edition supersedes which is typically every five years for SCIP products. Devices loaded with seed keying material are updated electronically through the rekey process. One year prior to a Universal Changeover (UCO), devices which are rekeyed electronically will be updated and contain a dual-edition key consisting of the current and next version. Failure to rekey a device supported by such prior to the expiration date of the key will result in the need to load the device or card with a new key.

Note: The KOK-22A KP FF Vector Set enables the creation and exchanging of credentials necessary to transfer and receive keying material electronically using a LMD/KP expires one year from the date generated. The FF Vector Set must be registered in LCMS as "Seed Key" and not operational key. If registered incorrectly, it will not be able to be updated through the KP Rekey process and will require a new key at the end of the one-year period.

g. When issued, modern key is moved and not copied like traditional electronic key with a register number of 00.

3. **CENTRAL FACILITY (CF) FORMS AND THEIR PURPOSE.** A matrix can be found on the following page which illustrates commonly used CF registration forms and their purpose.

a. Central Facility forms do not require a wet signature. They are considered signed when sent via digitally signed email or sent using DOD CAC Digital Signature via the Interactive Key Ordering or Registration Tool.

EKMS REGISTRATION FORM CHART

	COMMAND AUTHORITY REG. REQUEST (CF1201)	**U/R. REG. REQUEST (CF1206)**	**U/R DAO PRIV REG REQUEST (CF1207)**	**DAO REG. REQUEST (CF1202)**	**CLOSED PARTITION REG. REQUEST (CF1200)**	**U/R PARTITION PRIV. REG. REQUEST (CF1205)**	**Contact the COR**
ESTABLISH NEW USER REP. (MILITARY)		**X**	**X**	**X**			
ESTABLISH NEW USER REP (GOVT CONTRACTORS)	**X**	**X**	**X**	**X**			
MODIFY/DELETE USER REP INFO		**X**					
MODIFY/DELETE COMMAND AUTHORITY INFO	**X**						
ESTABLISH A NEW DAO CODE			**X**	**X**			
MODIFY DAO DESCRIPTION OR DELETE A DAO CODE				**X**			
MODIFY DAO CLASS **or** *ADD/DELETE CLASS 6 CODE PRIVILEGES*			**X**				
ASSIGN CLOSED PARTITION PRIVILEGE(s)						**X**	
ESTABLISH A CLOSED PARTITION					**X**	**X**	
MODIFY/DELETE COMSEC ACCOUNT INFO							**X**

The above forms, instructions and key ordering guidance can be found at https://www.iad.gov/keysupport. The Central Facility allows for key order forms to be submitted both electronically (online with use of a valid PKI) and manually (fax or email).

FIGURE AE-1

4. DEPARTMENT/AGENCY/ORGANIZATION (DAO) CODES.

a. A DAO code is a six-digit number which pertains to organizational descriptions and is assigned by the CF.

1. A DAO code is used to associate ordering privileges of User Representatives privileged to order modern keying material assigned the corresponding DAO code.

2. Existing COMSEC accounts already have one or more DAO codes assigned to them.

3. A DAO code is established by the CF upon receipt of a CF Form 1202 validated by the Command Authority. This form, as well as a User Representative DAO Privilege Registration Request (CF Form 1207) must be prepared by the COMSEC Account Manager or Alternate as User Representatives for the account.

4. Use of a DAO code is required on all key orders submitted for Iridium devices, KSV-21 cards and SCIP devices.

5. The CF has established predetermined DAO Codes for CCEB nations, NATO nations, and Coalition nations as identified on the applicable key order forms.

b. DAO Descriptions. New DAO descriptions for DON accounts require coordination and concurrence of the Command Authority. Naming conventions for DAO descriptions will be constructed as illustrated below.

1. Line 1: The first letters will be: MSC (Military Sealift Command), USCG (Coast Guard), USN (Navy), or USMC (Marine Corps) followed by the organizational title.

2. Line 2: Enter geographic location, or DEPLOYED, as applicable.

3. The below DAO descriptions will be used for DON accounts providing support to government contractors.

a. **For SCI Key:**
Line 1: GOVT CONTRACTOR
Line 2: Company Name

The geographical location of the company can be identified on line 2 if desired and space permits or such can be reflected in the “Additional ID” field on the key order form.

Note: The Command Authority of the sponsoring government organization under which the contractor is performing services on behalf of the government is required to sign the DAO registration request for a DAO description of "GOVT CONTRACTOR," if SCI key is required. The Command Authority is also required to sign the CF Form 1207 to authorize TOP SECRET privileges for the DAO Code and Class 6 Code "10" (i.e., SCI) for TOP SECRET privileges.

b. **For non-SCI Key:**

Line 1: <Company Name>
Line 2: <Geographic Location>

When adding a new DAO Code, request all required privileges, including the DAO and Class 6 Codes (if any) by entering the desired Class 6 Code and Ordering Classification Restriction Level (OCRL) on the CF Form 1207, DAO Privilege Registration Request. Do **not** enter more than one Class 6 Code in each block. Failure to request privileges in conjunction with the request to establish the DAO Code may delay receipt of key.

To ensure accuracy in processing when requesting more than one privilege, the EKMS ID must be reflected on the top of each continuation page (CF Form 1208).

c. DAO Code Modification and Deletion.

1. A CF Form 1202 must be completed which reflects "Modify" as the transaction type and submitted to Command Authority to modify a DAO code description.

2. A CF Form 1207 which reflects only the changed information, the name of the current Primary and Alternate and is annotated as "Modify" as the transaction type must be completed to and submitted to the Command Authority to modify a DAO privilege.

3. A CF Form 1202 which reflects "Delete" as the transaction type must be completed and submitted to the Command Authority to delete a DAO Code. Prior concurrence from other User Representatives with ordering privileges for the respective DAO Code must be obtained prior to submission of a CF Form 1202 as this will result in the deletion of all associated privileges (to include Class 6 Code privileges) associated with that DAO Code.

4. A CF Form 1207 which reflects “Delete” as the transaction type must be completed and submitted to the Command Authority to delete DAO privileges or a Class 6 Code.

d. Class 6 Code Privileges.

1. When placing a secure call, some user communities require additional authentication informed afforded through the use of a Class 6 Code.

2. Class 6 codes are uniquely and directly related to a specific DAO code although more than one Class 6 Code privilege may be associated with a single DAO Code.

3. User Representatives must be authorized key ordering privileges for specific Class 6 Codes.

4. The CF provides User Representatives and Command Authorities a printout which identifies all authorized privileges for DAO and Class 6 Codes.

5. Only one Class 6 Code with a particular DAO code is permitted per line.

6. When used, the Class 6 code description appears in the upper right hand corner of the far end terminal display next to the classification. SCI will only be displayed when both terminals are loaded with SCI keying material.

7. The use of Class 6 Code 10 (SCI) keying material is restricted to telephones or terminals located in spaces approved by the Security Manager or SSO for the discussion or processing of Sensitive C ompartmented Information (SCI) information normally is not appropriate for mobile phones.

8. DON accounts may order Class 6 Code 10 keying material at the SECRET or TOP SECRET level. Government contractors may order Class 6 Code 10 key at the TOP SECRET level only.

9. The most commonly used Class 6 Codes are illustrated below:

Class 6 Code	**Description Displayed**
10	SCI
15	RESDENCE (The missing “i” is due to display limitations)
30	WIRELESS

5. **DEFINITION AND RESPONSIBILITIES: COMMAND AUTHORITY, VALIDATION AUTHORITY AND USER REPRESENTATIVE.**

a. **Command Authority (CMDAUTH):** A CMDAUTH is defined as an individual responsible for the appointment and management of User Representatives for a department, agency, or organization (DAO) and their SDNS key ordering privileges.

1. Establishing User Representative accounts and appointing appropriate, trusted individuals as primary and alternates to provide SDNS key services to all users within the Command Authority's span of control.

2. Approving administrative modifications to the User Representative accounts they manage (e.g., personnel, administrative, and related POC contact information) by signing the User Representative Registration Request form.

3. Review and approval of new requests for a Closed Partition and Department/Agency/Organization (DAO) Code. Approval and management of related privileges through the verification and signing of appropriate registration request forms including modifications to existing Closed Partitions and DAO Codes.

4. Assisting User Representatives regarding submissions of DAO, Closed Partition Code and other related privilege requests to ensure required registration forms are properly filled out.

Note: Command Authorities do not review or approve key orders submitted by User Representatives and is not responsible for managing associated keying material generated and shipped to COMSEC accounts. Proper and timely submission of key orders and management of keying material are responsibilities of the User Representative, i.e. COMSEC Account Manager and Alternates.

5. Providing guidance related to modern key and related devices.

6. Assisting User Representatives in conducting their cryptonet reviews, when requested.

7. Assuming responsibility for the operational management of a Partition for a newly fielded system.

8. Authorizing cryptoperiod extensions when operationally

required, technically supported by the device and such is not expressly prohibited by the Operational Security Doctrine (OSD) for the device. This may be delegated to a Validating Authority, when such exists for the supported Closed Partition. Such extensions are limited to a maximum of 07 days. Extensions beyond 7 days require NSA approval and if discovered without such constitutes a cryptographic incident requiring reporting in accordance with Article 945 of this manual.

9. Maintaining accurate records on pertinent aspects of the cryptonet in sufficient detail to manage the membership of the cryptonet, assess the impact of, and recover from a compromise of the key. Such records must show the identity (and validate the membership) of all cryptonet members and the distribution authorities that support the cryptonet. Command Authorities may rely on a Validation Authority for this data if a Validation Authority is designated for the network.

b. **Validation Authority:** At the discretion of the Command Authority when a Closed Partition has two or more users at separate geographical locations, a Validation Authority may be established to review and validate ordering privileges on behalf of User Representatives.

1. The Command Authority may request the Validation Authority concur with the assignment of Closed Partition key ordering privileges for User Representative accounts. User Representatives may request help from the Validation Authority in managing the network's keys and providing advice on the operational and security aspects of the Closed Partition. The Command Authority, Validation Authority, User Representatives, and COMSEC Account Managers must work closely together to coordinate the secure handling of SDNS key assigned to each Closed Partition.

2. Validation Authorities **may not** order key but may perform one or more functions typically performed by a Controlling Authority for matters involving traditional (symmetric key) such as key tracking, compromise recovery actions, and cryptoperiod extensions.

3. The use of a Validation Authority is most effective for large Closed Partitions with many users of the same Closed Partition key. There is no benefit, purpose or use of a Validation Authority for matters related to Open Partitions.

4. The advantage to the Command Authority assigning a

Validation Authority is that the information is centrally controlled and the Command Authority knows all of the authorized user accounts. By having a Validation Authority report to a User Representative, the Command Authority loses visibility of those who receive key associated with the Closed Partition.

5. Validation Authority responsibilities would normally be fulfilled by a person attached to the operational organization directly supported by or most closely associated with the Closed Partition, or the organization that originally requested establishment of the Closed Partition. Upon request, the COMSEC Account Manager will advise the Command Authority/User Representative(s) who the Validation Authority is, by individual name or position. The Validation Authority must have sufficient knowledge of the requirement to be able to validate requests from users to join the net or to continue in the net.

6. COMSEC Account Managers can and may be required to provide advice to Validation Authorities regarding proper COMSEC procedures.

7. Validation Authorities for Closed Partitions are registered with the Command Authority and not with the Central Facility. A record message or digitally signed email may be sent to the Command Authority to establish a validation authority or affect a change to such as a result of transfer, separation, or reassignment of the incumbent.

8. A Validation Authority may be responsible for any or all of the following tasks:

a. Management of Closed Partitions identified as required by the supporting COMSEC account, User Representative or supported Command Authority.

b. Provide the Command Authority with concurrence or disapproval of requests by subsequent User Representative accounts to obtain ordering privileges for the Closed Partition. The Command Authority must authorize the privileges by signing the User Representative Partition Privilege request(s).

c. Understanding the operational requirements supported by the Closed Partition and being familiar with the operation, capabilities, and Operational Security Doctrine (OSD) for the supported equipment.

d. Advising the Command Authority and User

Representative(s) promptly when there is a change of personnel performing the Validation Authority function.

e. Notification of all Closed Partition key holders and the supporting User Representative(s) of any changes in the network structure or keying material status.

f. Requesting classification changes through the appropriate User Representative(s) and Command Authority. The Command Authority will validate such through submission of a User Representative Partition Privilege Registration Request to the CF.

g. Maintaining accurate records identifying end users of the Closed Partition and assessing the impact of, and recovering from a compromise.

h. Contacting Closed Partition users at a minimum of annually to identify the keying material and provide holders with valid contact information for the Validation Authority during and outside normal business hours.

i. Authorizing cryptoperiod extensions consistent with the guidance contained in paragraph 5.a above.

c. **User Representative (UR):** A UR is defined as the Key Management Entity (KME) authorized by an organization and registered by the CF to order modern key. User Representatives are authorized to order modern keying material, provide information to key users and must ensure the correct type of key is ordered. The User Representative is typically, but not always, the COMSEC Account Manager or Alternate(s). Duties of a UR include:

1. Completing, signing, and submitting SDNS keying material order requests for all users under their purview.

2. Communicating with net planners and users, as necessary, to identify keying material requirements accurately.

3. Accurate and timely submission of keying material orders to ensure routine and urgent keying material requirements are satisfied and ensure replacement key is received and issued prior to the expiration of key held/issued by the account.

Note: Failure to identify and order modern key prior to the expiration of currently used key results in both

service interruptions and COMSEC incidents related to use of expired (superseded) key and is preventable.

4. Coordinating with each COMSEC Account Manager involved, prior to submitting key orders.

Note: Supported Local Elements MUST inform the COMSEC Account Manager as soon as possible when a Closed Partition will be established and identify the key and classification required. The COMSEC Account Manager cannot obtain the key if the appropriate documentation is not completed, submitted and approved by the Command Authority.

5. Requesting, through the use of the appropriate registration forms and approval of the Command Authority approval establishment of new DAO Codes, associated privileges, Closed Partitions and related ordering privileges.

6. Initiating annual reviews of keying material by contacting cryptonet members. At a minimum, User Representatives will identify the keying material and advise net members on how to contact the User Representative under normal and emergency circumstances. User Representatives shall conduct periodic reviews of fielded keying material in Closed Partitions to confirm Partition structure, holders, and quantities held to meet operational requirements, as well as each user’s continuing requirement for the key. If a Closed Partition is no longer required, the User Representative must, using the appropriate registration request, advise the Command Authority to delete the Partition and advise all holders upon approval. Command Authorities may require a report of the User Representatives’ periodic reviews.

6. **OPEN AND CLOSED PARTITIONS.** A partition represents a division of users or a Community of Interest (COI) which communicates securely within the COI through the use of SDNS universal keying material. Any person reflected on the commands CF Form 1206 which has been validated and submitted by the Command Authority and processed by the CF can order Open Partition keying material.

a. Open Partition key is used in a variety of networks and link encryption equipment. Currently, two Open Partition codes exist:

(1) 0000032793 for operational key applications, and
(2) 0000032795 for test key applications.

Open Partition privileges and privileges for the Closed Partition 0000055555 used for U.S. COI Closed Partitions for STE and SCIP products are automatically assigned to new User Representatives by the CF.

> Privileges for the other STE/SCIP COI Closed Partitions (CCEB = 1400200001, NATO Nation = 1550200001, Coalition = 1601300001) and the Iridium Closed Partition (0000050000) will be automatically assigned by the Central Facility as key orders are submitted.

b. Closed Partition key consists of an exclusionary subset of SDNS keys formed in a single key signature universal used to permit communications among elements within a specific Closed COI.

c. In addition to the CF Form 1206, the ordering of modern keying material used for Closed Partitions requires the commands User Representative submit a User Representative Partition Privilege Registration Request (CF Form 1205) to the Command Authority or Validating Authority, as applicable.

> **Note: The CF will not accept registration forms not validated by the Command Authority or Validation Authority, as applicable.**

d. Although DIRNSA is reflected on the Master Reference Catalog (MRC) as the Command Authority for all modern keys, DIRNSA does not validate User Privileges; the Command Authority/Validation Authority for the network does so. A listing of modern key Short Titles NCMS is the Command Authority will be posted on the NCMS CAS portal. If the Command Authority is other than NCMS and cannot be identified, COMSEC Account Managers should contact the Central Facility at 240-273-1480 (commercial) or 1-888-342-0902 (toll free) or the NCMS Key Division at 240-857-9085 for assistance.

e. Modern key is ordered online using the CF interactive online ordering tool and submission of the applicable order form by an authorized User Representative. The use of digital signatures in lieu of wet signatures are permitted for CF forms.

f. This same concept which applies to physical segmented off-the-air test or maintenance key applies to modern key. Modern test key may be used indefinitely beyond the expiration date if the equipment such is used in supports such. The load and destroy concept discussed in paragraph 8.c below does NOT apply to test key and test key can remain stored in the DTD, SKL, TKL, etc… as long as required.

7. **ORDERING OPEN OR CLOSED PARTITION KEY.**

a. To order modern keying material requires privileges approved by the Command Authority and validated by the CF.

b. Changes related to ordering privileges, i.e. additions, deletions or modifications must be communicated via the Validation Authority or Command Authority, as applicable to the CF via a properly completed and digitally signed CF Form 1206. When completing the CF Form 1206, to ensure there is enough space available to enter all personnel use first initials instead of first names.

c. Orders are submitted via the Interactive Key Ordering Tool on the https://www.iad.gov/keysupport web site.

d. Previously used User Representative (UR) numbers are not accepted for key orders. Current procedures require the use of the commands EKMS account ID on modern key orders.

e. To order Closed Partition Keys requires a CF Form 1206 **and** CF Form 1205 be on file at CF for the short title required. It must be understood, to maintain visibility on holders of key under their management and purview, some Command Authorities including but not limited to CENTCOM, CPF, JCMO do not allow User Representatives to order keys under their purview from the CF. For questions related to privileges for ordering modern key, please contact the respective Command Authority, NCMS or the CF.

NOTE: Completed Key Orders, CF Form 1205 and CF Form-1206 will be maintained in accordance with Article 706.a.9 and Annex T.

f. For CENTRIXS Short Titles managed by COMPACFLT, COMSEC Account Managers must consult their ALCOMPAC P and ALCOMLANT Alfa general messages for additional guidance in obtaining ordering privileges for these Short Titles. Failure to do so may delay the fulfillment of orders for mission essential keying material.

g. Procedures for ordering keys for the CENTRIX are located on the JCMO website. See Annex S for the URL for the JCMO website.

h. Orders for new copies of modern keys can be submitted as required. It is recommended that orders for new keys be submitted a minimum of 30 days prior to the expiration of the current keys held at the COMSEC account. For deploying units it is recommended that key orders be submitted and new keys downloaded prior to departure so a ready supply of keys is available for the duration of the deployment.

i. If the User Representative does not know the Command Authority of a partition they can contact Central Facility at 240-373-1480.

8. **MODERN KEY: ACCOUNTING, CRYPTOPERIODS, DESTRUCTION, MANAGEMENT AND USAGE.**

a. Accounting. Modern keying material from the CF is accountable to the COR as ALC-6 material (EKMS FIREFLY and MSK received on a KSD-64 are ALC 1 accountable).

1. When modern keying material is received from the CF, the recipient must wrap and submit the receipt to the CF (account 880103) and the accounts Primary Tier 1 segment (PT1S).

2. Failure to submit receipts or respond to a tracer notice in a timely manner may result in the keys being placed on the Compromised Key List (CKL) which will result in a denial of service to the client node device in which the key is loaded and will prevent electronic rekeys and seed key conversions.

3. COMSEC accounts in receipt of a tracer notice for material received in which the receipt was submitted should contact the NSA POC reflected in the tracer notice via email or phone at (301) 688-8110 or DSN 644-8110.

4. In addition to normal accounting for the modern keys via the EKMS account, it is recommended that User Representatives track the expiration date of their modern keys out of band. A "Modern Key Tracker" tool is available for download via the NCMS SIPRNET website. The User Representative can also use electronic calendar reminders for modern key ordering dates and modern key expiration dates (the expiration date of a modern key is not classified)

b. Cryptoperiods.

1. Operational modern key expires/supersedes one year from the date it was generated, not from the date downloaded via the message server, issued or loaded. User Representatives can use the originator transaction date on the receipt for the generation date (e.g. if a key was received on 15 AUG 14 it will expire 31 Aug 15).

2. Seed keying material commonly used for devices which support updating through the rekey process supersedes every 05 years in what is referred to as the Universal Changeover (UCO).

3. Use of keying material which has expired/been superseded is a cryptographic incident reportable in accordance with Article 945 unless the cryptoperiod was extended by the Command Authority or Validation Authority, as applicable. Such extensions are limited to a maximum of 07 days in accordance with Paragraph 5.a above.

4. Traffic Encryption Key (TEK) is typically automatically generated every 24 hours in the form of a session key by SDNS equipment on full time circuits/networks. For equipment not possessing the ability to generate a new session key every 24 hours, the operator must manually perform an update every 24 hours. Unless prohibited by the Operational Security Doctrine (OSD) for the device, the TEK cryptoperiod may be extended up to a maximum of 72 hours for holiday weekends.

5. The discovery of devices operating on expired key or in which the TEK was not manually updated as discussed above both constitute an unauthorized extension of a cryptoperiod and must be reported in accordance with Article 945 herein.

6. Devices which make use of Seed Key are updated through the electronic rekey process. One year prior to a UCO, a successful rekey will result in the device containing dual-edition keying material consisting of the current and next universal.

c. Destruction.

1. Successful loading and conversion of Seed Key is reflected in a Key Conversion Notice (KCN) received via the Message Server from the CF. Destruction reports are not required for Seed Key successfully converted but are required for failed conversions or destruction of unused Seed or Operational Modern Key.

2. The concept of premature destruction does not exist regarding Modern or Seed keying material. However, when destroyed, the destruction must be reported to the COR. User Representatives do not need Command Authority approval to destroy modern keys prior to expiration date.

3. Inadvertently destroyed Modern or Seed keying material is not resupplied by CMIO, NCMS or NSA. Resupply can only be accomplished through submission of the required key order forms by the COMSEC Account Manager, Alternate or other individual authorized User Privileges at the CF.

4. Test keying material (USFZU 0000032795) for SDNS devices is not authorized for use on operational circuits and does not supersede/expire like operational keying material. In the same manner as physical segmented test key, such may be stored in an electronic storage device (DTD, SKL, TKL, etc…) and used indefinitely beyond the expiration date.

5. When loaded, LE personnel will verify the supported network is operational, delete the modern key loaded from the electronic storage device (DTD, SKL, TKL, etc… storing such) and provide a manually generated (SF-153) destruction report to the supporting COMSEC Account Manager. Block 13 of the report will include the serial number of the device the key was loaded in.

6. The COMSEC Account Manager will use the destruction report signed and submitted by the LE to record the item as "Filled In End Equipment" in LCMS. Although a working copy of a destruction report is not created by LCMS in this scenario, the keying material will appear on the next consolidated destruction report originated by the account.

7. If a LE is issued an electronic storage device such as a DTD, SKL, etc… which fails or becomes corrupted, the LE will submit a statement to the supporting Account Manager which includes; the date/time of the failure, the serial number of the device and any errors displayed, if any. If the device is storing modern key not previously loaded and destroyed, the modern key CANNOT be reissued as it is KMID unique.

Although Traditional (Reg 00 key) may be reissued, the Manager must provide the LE personnel with a destruction report for the keys lost due to the device failure or corruption. When signed and returned, the COMSEC Account Manager will record the items as destroyed in LCMS so the Modern Keys do not remain charged to the account. This will also ensure LCMS accurately reflects the correct quantity for Traditional Key held by the LE, when reissued. The Manager will have to perform a LE Physical Material Return to assume responsibility for the failed device and have such reflected as on-hand at the account level and issue a replacement storage device and issue replacement modern and/or traditional key, as applicable.

> **Note: If possible to do so, the Manager will upload and review the audit trail data when the device is turned in, log the review in the audit trail review log, zeroize the device (for SKLs, enter the SSO password incorrectly 10 times) to delete the LKEK/HDKP. Contact SSC Atlantic for assistance to determine whether disposition instructions will be required for the device or if it can be returned to service at the account level, with assistance.**

d. Management and Usage of Modern Key.

1. Modern key is register/serial number specific and is uniquely identified by the associated Key Management Identifier (KMID).

2. Loading more than one ECU with a modern key having the same KMID previously loaded is **prohibited.** The discovery of such in other than a COMSEC emergency constitutes a cryptographic incident in accordance with Article 945 herein.

3. To provide for redundancy should a device fail and require reload outside normal working hours, adhering to proper local custody procedures, it is highly recommended COMSEC Account Managers issue a minimum of 02 modern keys at a time to LE personnel for each supported network/system.

4. Modern key will not be copied from device to device at the account or LE level to prevent reuse, use in another device, late destruction or the discovery of the key to still exist after being destroyed and reported as such as required. To mitigate the potential associated with a DTD, SKL, TKL, etc… failure and loss of key, it is recommended COMSEC Account Managers issue spare copies of required modern key with different KMIDs to a secondary storage device, which will be issued adhering to local custody procedures if a secondary device is not currently held by the LE.

5. Voice devices communicate at a common level. If the person at site “a” is using a terminal keyed at the Top Secret level but the person at site “b” is using a terminal keyed at

the Secret level, the highest classification of information passed must be restricted to the common level which in this illustration is Secret.

6. Unlike secure voice devices, data devices such as In-Line Network Encryptors (INEs) or High Assurance Internet Protocol Encryptor (HAIPE) devices do not operate at a common level. Sites using keying material of a differing classification that required for the network will not be able to communicate.

7. Except in an operational emergency, authorized by the units Commanding Officer, modern key will not be transferred between accounts without authorization from the Validation Authority or Command Authority, as applicable. Should an operational emergency exist which could disrupt critical communications necessitating the local CO authorize an emergent transfer of Closed Partition modern key, the transferring COMSEC Account Manager must report the transfer to the Command Authority and the COR within 96 hours from the transfer.

Note: Failing to order and maintain an adequate allowance of modern key for supported networks/enclaves is not considered an operational emergency. An operational emergency would be when the account cannot receive the required key due to a LMD/KP failure or when the accounts FF Vector set and related credentials have expired. In the later scenario, the command requiring the key would not be able to receive it through the X.400 (message server) until a new FF Vector Set is received, loaded and new credentials posted. The only way to receive the key would be via fill device from the providing account, if possible or via Over-The-Air-Distribution (OTAD).

8. HAIPE-to-HAIPE Key Transfer (HTHKT): Is a process supported by many modern ECUs which permits a Net Control host device to distribute modern key to client HAIPE devices.

a. The same KMID will NOT be distributed to more than one client HAIPE device.

b. Using the log illustrated in Annex R to this manual, the Net Control site transferring the key(s) will document the electronic transmission in an Over-The-Air-Rekey (OTAR) log in accordance with Article 1182 of this manual. OTAR and OTAT logs will be retained in accordance with Annex T herein.

c. Although extraction of key is not possible from a client HAIPE device updated through the HTHKT, recipients will use and retain an OTAR log described above to maintain awareness as to the expiration date of the key received to prevent use of expired key and the reporting of such as a cryptographic incident.

9. **MODERN KEY OPERATIONS WITH ALLIED COUNTRIES.**

a. For strictly U.S. networks, a U.S. only key will be used.

b. For networks which include foreign nationals, i.e. CCEB members, allied countries, etc… in which the foreign nationals will be in physical control/responsibility of the keying material or equipment, an allied key is required.

c. For networks which include foreign nationals, i.e. CCEB members, allied countries, etc… who only have access to data or information from the network but do not have physical control/responsibility for the keying material equipment a U.S. key may be used.

d. Access to classified information must be restricted to the levels set forth in the National Disclosure Policy (NDP-1) and controlled, managed, and safeguarded in accordance with DODD 5230.11, SECNAV 5510.34(series), SECNAV 5510.36(series) and the DON Foreign Disclosure Manual.

e. The release of COMSEC materials to a foreign government must be approved in accordance with Article 505.j, CNSS-1002, and CNSSP-8.

10. **INCIDENT REPORTING.**

a. COMSEC incidents involving modern key must be reported to the Validation Authority or Command Authority, as applicable and the supporting COMSEC Account Manager applicable.

b. The COMSEC Account Manager is responsible for proper and timely reporting set forth in Articles 930, 940, 960 and 970 of this manual. For incidents which involve an external LE and the related LOA/MOU stipulates the LE will report the incident, the LE is responsible for reporting the incident in accordance with the aforementioned articles and will include the Plain Language Address (PLA) of the supporting account as an info addee on the incident report. See Articles 965, 970 and Figure 9-2 for required PLAs and content.

Note: For incidents involving modern key, the Command Authority is required in lieu of a Controlling Authority which does not exist for modern key.

c. The KMID of the keying material MUST be included in incident reports related to modern keying material so such key can be placed on the Compromised Key List (CKL).

11. **COMPROMISE RECOVERY.**

a. When evidence exists that an SDNS key has been compromised, immediate action must be taken by the Command Authorities or Validation Authorities, as applicable COMSEC Account Managers, the Service Authority and NSA in accordance with the Operational Security Doctrine for the equipment.

b. The following compromise recovery options are available and listed in order of preference:

1. Report the incident as discussed in Paragraph 10 and Article 945 of this manual. This will bring to the attention of NSA to place the effected KMID on the CKL list excluding the holder of the compromised key from the cryptonet.

Note: The User Representative must issue or order a new key for the same Partition as the compromised key to enable that user to rejoin the net.

2. In extreme circumstances, the compromise may require replacement of all keys in the Closed network/Partition and result in the need to create a new Closed Partition to replace the Partition containing the compromised key.

Note: In the second option above, this will require the Command Authority to submit the required registration requests to add a new Closed Partition and Partition privileges for authorized User Representative accounts. Provisioning to Allies may take longer and operations should be suspended until key is distributed.

3. Continued use of the compromised key is a last resort and should only occur when keying material changes would have a serious detrimental effect on operations or when no means exist to obtain replacement material. In this scenario, the Command Authority or Validation Authority, as applicable must notify all Partition holders and supporting User Representatives (by other

secure means, if available) of the possible compromise and direct net members (users) to minimize transmissions to the holder of the compromised KMID.

12. **GUIDANCE FOR DEPLOYABLE UNITS.**

a. It is paramount that the Manager and each Alternate have ordering privileges at the CF. In preparing for deployment, commands should review their account holdings prior to deployment and order enough copies of the modern keys to support operational requirements throughout the deployment.

b. When modern keys are loaded into End Crypto units (ECUs), LE personnel must provide a manual destruction report to the COMSEC Account Manager. The COMSEC Account Manager must record the item in LCMS as “Filled in End Equipment” and submit the reportable destruction report reflecting the key loaded to the COR, as required.

c. Keys not loaded prior to the expiration date must be destroyed and such reported to the COR.

d. Ensure the Manager and a minimum of one Alternate has ordering privileges. It is recommended additional alternates, up-to the number permitted by the CF have ordering privileges. When either the Manager or an Alternate is replaced, a new CF Form 1206 must be submitted as discussed herein to enable the newly appointed person to order modern keying material.

e. Review the applicable OPTASK COMMS, OPTASK LINKS and other messages which outline communication requirements to know in advance what modern key is required. This is especially important if the material required is not currently held or applicable privileges have not been established and it is for a Closed Partition.

f. Order a minimum of (10) copies of each modern key when submitting orders. Remember, the use of operational modern key is based on a load and destroy concept. The particular KMID loaded is not to be used on another ECU or retained in the DTD, SKL, TKL, etc… following loading and verification the supported circuit is operational.

g. Rekey all STEs, the KOK-22A, and other devices supported through the rekey process while in port. Although it can be done at-sea, at times communications restrictions such as EMCON, River City, or other bandwidth limitations, etc... may make such impossible or difficult to successfully do.

h. Prior to deployment, ensure your FF Vector Set for the KOK-22A (KP) is rekeyed and updated credentials are posted to the Directory Server. Should a units FF Vector Set expire and their credentials are outdated, the unit will not be able to generate credentials required to send and receive electronic keying material from the LMD/KP until a new FF Vector Set is requested in accordance with Article 670, received and loaded.

Note: FF Vector Sets are no longer delivered on KSD-64As and are delivered electronically. If an accounts FF Vector Set expires, the account will have no way to receive a new FF Vector Set and will have to reflect another six-digit account number on the order to have the key placed in the other accounts X.400 mail box. This will require the receiving account to register the unit with the expired FF Vector Set as a LE and issue the key on a local custody basis in a DTD, SKL, etc… If the receiving account is not located in the same vicinity, the account identified to receive the FF Vector Set may have to coordinate an Over-The-Air-Distribution (OTAD) via SKL/STE with the requiring unit to deliver the replacement FF Vector Set.

i. Do not rekey a KP with unprocessed Bulk Encrypted Transactions (BETS) on the LMD desktop. Doing so will prevent the material from being unwrapped and processed and require reporting under Article 742 of this manual.

j. Procedures for conducting a KP rekey can be found in the EKMS 704 (LMD/KP Operations Manual).

k. For modern key which has been inadvertently destroyed or is lost as a result of a LMD/KP failure, the COR cannot effect resupply for the unit. The COMSEC Account Manager must order replacement of the key through the interactive portal as discussed in Paragraph 6 above.

Annex AF

SIMPLE KEY LOADER (SKL) WITH EMBEDDED KOV 21 CRYPTOGRAPHIC CARD

1. **Purpose and applicability**: To provide guidance for EKMS Managers and LE personnel in the accountability, safeguarding, and handling of the AN/PYQ-10 Simple Key Loader (SKL).

2. **SKL System Description/Use**:

a. The SKL is a Controlled Cryptographic Item (CCI) that is accountable to the Central Office of Record (COR) as an ALC 1 item.

b. Although the serial number of the SKL is displayed on the outside label, the serial number of the embedded KOV 21 cryptographic card is not displayed on the outer shell/label. The KOV 21 when used in the SKL application must never be removed from the SKL casing to verify its presence for initial receipt or inventory purposes. Its presence will be assumed on the basis of its continuing operation.

c. The SKL is the next generation data transfer device that emulates the KYK 13, KYX 15, and KOI 18 electronic functions and is backwards compatible with the Data Transfer Device (DTD) or AN CYZ 10.

d. The SKL has a host side and COMSEC side. The host side of the SKL can also encrypt and store information and data. Encrypted key extracted from the SKL passes from the host side through the COMSEC side for decryption.

e. Like the DTD, the SKL employs a crypto ignition key (CIK); however, to access keying material (keymat) and host side data as well as initiate security functions, the authorized user must perform a successful logon (insert CIK ***and*** enter User Password). Unlike the DTD, each SKL makes use of only ***one*** CIK. In other words, all Users of a particular SKL will share the same CIK. Additionally, the SKL ***cannot*** segregate COMSEC material by User. Accordingly, a successful logon (use of CIK and password) gives the User unencrypted access to ***all*** the keymat and info stored on the SKL.

f. The SKL is operated as a limited keyboard device and the nomenclature is “AN PYQ 10 C”.

g. The SKL is an important COMSEC Account Manager tool and component of the Electronic Key Management System (EKMS) as it is used to securely distribute keymat from the Local Management Device and Key Processor (LMD/KP) to Users. It can fill key to an end cryptographic unit (ECU) or fill key to a DTD, SDS, SKL, or to a LMD/KP.

h. The SKL has more functionality than the DTD in that it matches DTD capability without the use of multiple CIKs. Benefits: Single CIK concept and storage of encrypted keys for long periods of time on the SKL’s host side.

3. Maximum Level of Operation/Use:

a. The SKL host side is authorized to store Secret-high information/data.

b. The SKL host side is authorized to store keymat of all classification levels and categories that have been Type-1 encrypted.

c. Keymat will not be stored longer than one year in the SKL without Controlling Authority authorization.

d. All SKLs will contain only NSA-approved user application software (UAS).

4. Personnel/Access Controls/Two-Person Integrity (TPI) Requirements/Physical Security Requirements:

a. The integrity of information and keymat secured in the SKL must be overseen by a “Site Security Officer” (SSO) who may also be the COMSEC Account Manager or a designated Local Element Issuer/User. The person filling this role grants User access to the SKL, ensuring that all persons granted User status are cleared to the level of keymat and information in the SKL.

> **NOTE: Unrestricted access to the SSO account/password must be limited to those who are authorized to perform all of the privileges allowed by having access to the SSO account/password.**

b. The SKL is considered unclassified when it does not have its initialized/associated CIK inserted and said CIK is stored separately and appropriately per the highest classification of keymat or data stored in the SKL.

c. TPI handling is required when the SKL is storing Top Secret keymat and its initialized /associated CIK is inserted or can be readily accessed. The SKL reverts to unclassified CCI when its initialized/associated CIK is not inserted and said CIK is stored under TPI storage protection.

AMD-9

d. There will be a maximum of 11 Users per SKL (one SSO with up to 10 additional Users). The ***single*** exception to this policy: shift work environments (e.g., watch stations) where, owing to numerous shift workers, it is necessary to appoint more than one SSO per SKL and to allow the sharing of passwords among members of a given shift. To ensure proper compliance with this policy exception, these commands/activities will maintain an access list of personnel authorized access to/knowledge of the ***shared*** User password for a given SKL. This can be accomplished in any of the following ways: using a watch station bill tailored for this purpose or by a separate access letter that links the serial number(s) of the SKL with a particular shift worker group. These documents must ***not*** include the User Password to the SKL; they are subject to review during ~~formal COMSEC Account inspections~~ COR Audits~~. and Advice and Assistance Team Visits.~~

e. A combination of CIK, Username and password allows access to all information and keymat secured in the SKL.

f. While logged on to the SKL (and coincidentally to the KOV 21 cryptographic card), Users must maintain accountability of the SKL. When the green LED indicator is steady, the User is logged in. Users should seek to minimize the amount of time they are logged in to the device to an amount reasonable to perform job functions. When logging off the SKL (and coincidentally off the KOV 21 card), Users must power down the entire device immediately.

g. Users must log off the SKL at the end of their authorized transaction or shift.

h. Users of the SKL will check the SKL housing for casing damage or cracks at least weekly or at next opening of the security container for a non-watch environment and will simultaneously verify the serial number of the SKL to be certain that it is the SKL they were issued.

i. If a SKL is released to a foreign partner and comes under their control for any period of time, that device may not be returned to the U.S./Department of Navy (DON) equipment inventory. DON accounts shall not accept receipt for such devices (this includes the embedded KOV 21 cryptographic card) but should instead contact NCMS N3 and request disposition instructions.

5. **CIK HANDLING/CONTROLS**:

a. The SKL contains one CIK port. All Users of a particular SKL will share the same CIK.

b. When the CIK is inserted and with proper Username and User Password authentication, the information and keymat can be accessed by the SKL operator in the format in which the keymat was loaded.

c. The CIK by itself is unclassified but is locally accountable to the COMSEC Account Manager by quantity. Because each SKL makes use of only one CIK, sight inventories performed by the COMSEC Account Manager or Alternate or other designated person will include sighting the assigned serial number of the SKL and the authorized User will then be asked to insert the CIK and logon. A successful logon is confirmation of the correct CIK/SKL association however, for account inventory purposes, CIKS associated with initialized or issued SKLs will be reflected on a locally generated SF-153 by quantity as illustrated below.

Short Title	**QTY**	**Beginning**	**Ending**	**ALC**
SKL CIK	# of devices initialized/issued	NA	NA	NA

Note: There is no inventory requirement for CIKS for uninitialized or unissued devices. Whether initialized or not, the SKL itself however, is a ALC 1 item and must always be accounted for by serial number.

d. When the SKL is unattended, remove the CIK and store securely and separately from the SKL to avoid stringent safeguarding measures. The SKL with initialized/associated CIK inserted is considered classified commensurate with the highest classification of keymat or host side data the SKL is storing.

e. When the CIK is removed from the SKL in order to lessen SKL handling requirements, store the initialized/associated CIK in a security container commensurate with the highest classification of the keymat or data stored in the SKL. Also ensure that only those authorized use of the particular SKL have access to or knowledge of the combination to the security container.

f. **Lost CIKs** must be promptly deleted from the associated SKL. See Paragraph 15.a.2 and the associated note for additional information regarding criteria and reporting.

g. Failure to inventory in-use/associated SKL CIKS must be documented in accordance with Article 1005.a.

6. User Password(s):

a. User Passwords are UNCLASSIFIED but sensitive and, if written down, must be stored in a locked drawer or security container restricted to access by an authorized User. A central record of passwords may be maintained as discussed in paragraph 6.g. below.

b. The Password must contain anywhere from 6 to 12 alphanumeric, case-sensitive characters.

c. Selection of the Password must follow good security practices such as those found in the DoD Password Management Guideline (CSC-STD-002-85).

d. The SKL will allow for up to 10 consecutive failed attempts to log on. After the tenth unsuccessful attempt, the User will be locked out and will have to be reinstated by the SSO. Should the SSO fail on the tenth attempt to enter the correct username or password, the SKL will automatically reset/zeroize, and delete all Users, keymat, and data. Once this function is completed, the SKL will prompt the SSO to log on, and all mission data and keymat must be reloaded.

e. Except as indicated in paragraph 4.d. of this document, the sharing of Passwords is prohibited and access to a SKL must be set up as one User per Password.

f. The Password must not be written on or affixed to the SKL. Further, because the audit info within the SKL is segregated by individual User, it is strongly recommended that all Users record and appropriately safeguard their Passwords to prevent unauthorized access/use.

g. A central record of the Passwords may be maintained in a single security container providing each Password is recorded, sealed, and wrapped by the authorized Password holder. Article

515 guidelines for wrapping as these support ready identification of tampering efforts by unauthorized personnel. Procedures must also include the use of the SF 700 Security Container Form and a logbook for maintaining a record of when and by whom Passwords are accessed. Additional protective measures may be established by the SSO or COMSEC Account Manager to control access to User Passwords.

7. <u>Keying Information/Cryptoperiods</u>:

a. Local Key Encryption Key (LKEK) and the Host Data Protection Key (HDPK):

(1) Upon CIK initialization, during which the randomization process associates and allows access to a particular SKL, two split keys are created: LKEK and HDPK. These keys perform the encryption and decryption for the SKL. More specifically, the LKEK encrypts/decrypts keymat while the HDPK encrypts/decrypts info or data stored on the SKLs host side.

(2) During CIK initialization, only the splits are stored on the CIK.

(3) When re-initializing the CIK to create a new LKEK and HDPK, the keys previously protected by that CIK are unrecoverable unless they have first been moved to another device.

(4) The LKEK and HDPK have a cryptoperiod of one year and must be superseded at that time. This is accomplished by re-initializing the SKL and its associated CIK, yearly.

(5) **Documentation must exist to verify reinitialization of SKLs occur annually.** This can be accomplished by uploading and printing the audit trail after initializing/reinitializing a SKL or through adding a column and recording such in the Audit Trail review log. A sample log for both reinitialization and Audit Trail reviews can be found on the NCMS CAS portal.

b. Transfer Key Encryption Key (TRKEK):

(1) This key encrypts keymat when transferred from one device to another via STE or other approved device (from a LMD/KP to a SKL, or from one SKL to another SKL or SDS or DTD). The encrypted key is stored on the host side in the

SKL in a super-encrypted mode. The TRKEK must be filled to the receiving SKL to permit the SKL to decrypt the key for use. The encrypted key is stored on the host side in the SKL in a super-encrypted mode until decrypted for red (unencrypted) output.

(2) TRKEKs must be pre-placed in the receiving SKL. Except in an emergency, TRKEKs must not be sent via STE secure mode in unencrypted form. A maximum of one year's worth of TRKEKs may be preplaced.

(3) TRKEKs must be classified to the highest classification of key they encrypt.

(4) Use a three-month cryptoperiod when the TRKEK is used in a large net, or its associated encrypted key is transmitted via secure means other than a STE or other approved device.

(5) Use a one-year cryptoperiod only when the TRKEK is used in a small net (e.g., within one COMSEC Account), and its associated encrypted key is transmitted via a STE or other approved device.

NOTE: The one-year LKEK and HDPK cryptoperiods limit the amount of time a TRKEK may be used to one year, since the SKL CIK must be re-initialized yearly in order to form new LKEKs and HDPKs. The same procedures must be followed to reinitialize a SKL as those performed to initialize the device. Step-by step procedures can be found on the NCMS CAS portal. Key stored in the device should be transferred to another device <u>prior to</u> reinitialization or all key will have to be filled/issued again.

c. NATO keymat handling:

(1) Per SDIP 293, imported or electronically distributed NATO keymat will be handled by the SKL like U.S. keymat while being distributed in the EKMS.

(2) SKL operators must check the short titles to ensure proper handling because this keymat will not carry NATO classifications while in the SKL, only U.S.-equivalent classifications. This is especially important when both NATO and U.S. keymat are in the same SKL at the same time.

8. **Keymat Control Requirements**:

a. Loading physical key:

(1) The Controlling Authority may authorize the following options:

(a) Single segment loading of key, per short title, with the unused segments remaining in the canister until they become effective,

(b) Loading of a full canister/edition of keymat, to be loaded into the SKL at one time. The latter option is permitted with the understanding that the Controlling Authority accepts the risk of having to supersede an entire edition of key should a compromise occur. The Controlling Authority must specifically authorize this option.

b. Loading limitations:

(1) No more than one canister (edition) of keymat per short title will be held in the SKL at any one time.

(2) No more than 12 months and one spare month will be held in the SKL at any one time.

(3) Single authorized exception to one-canister rule per SKL: Follow-on canister of keymat may be loaded into the SKL at any time during the final month of the previously loaded and still current edition’s effective period.

c. Retention of pulled keytape segments outside of the canister is discouraged to the extent possible. Where this cannot be avoided, secure extracted keytape segments according to classification level until superseded; then destroy in accordance with Article 540.

d. Physical keymat converted to electronic form and loaded into a SKL:

(1) May be subsequently imported from the SKL to the LMD/KP and stored there until supersession or re-issue to the SKL, if necessary.

(2) When physical keymat is loaded into the SKL and then imported into the LMD/KP, the short title is changed in the LMD/KP to reflect the changed format from paper to electronic. The electronic and physical keymat are compatible but it complicates matters to have to account for the same keymat by different short titles. The Controlling Authority for the paper version of a Short Title also serves as the Controlling Authority for any electronic version of the keymat.

e. Transferring keymat between devices:

(1) Keymat encrypted (black) by a SKL TRKEK may be transferred between SKLs on circuits secured by STE or other approved devices.

(2) Unencrypted (red) keymat may be transferred between SKLs that are connected by STE or other approved device in the secured mode; this assumes the communicating STE or other approved device and all operators are authorized/cleared to pass information to the classification level of the transferred keymat.

(3) TRKEK replacement for remote activities: Supporting COMSEC Accounts (LMD/KP) may transfer new TRKEKs via over-the-air (OTAT) to remote Local Element (LE) activities. The remote LE must have at least two SKLs having different TRKEKs that supersede on different dates. The supporting account can transfer new TRKEK for one of the remote LE's SKL to another of its SKLs. The remote LE can extract the new TRKEK from the "receiving SKL" and fill it into the "using SKL." This practice can continue indefinitely.

(4) Important security cautions regarding keymat transfers:

(a) A NSA-approved adaptor/connector (RS232 cable) must be used between the STE and SKL to effect transfers. Do not attempt transfer using a non-approved adaptor/connector. The transfer of unencrypted keymat (red) using a non-approved adapter/connector is a reportable COMSEC incident.

NOTE: For information on how to obtain an approved cable, contact SPAWAR Systems Center Charleston (SSC) at (757) 558-6694.

(b) The SKL battery eliminator must **not** be used during key transfer. [**NOTE**: The battery eliminator is designed to reduce battery cost during high energy functions such as software downloads and training. Its use, however, is **not** approved for use during key loads and transfer evolutions. The prohibition stems from the fact that the battery eliminator is not TEMPEST approved.]

f. **Local Custody, Accountability, Safeguarding, Inventory, Destruction, and Database Corruption requirements:**

(1) Local custody issue. Recipients of either a SKL or of key issued in a SKL from a LMD/KP or loaded via hard-copy key and a legacy fill device (KOI-18) will acknowledge receipt of the key by signing local custody documents containing the accounting information minimally required by EKMS 1 (series), Annex Z, paragraph 13.d. For additional information related to the issuance of electronic key in a fill device (includes KYK-13, KYX-15, DTD, SKL, etc…) and documentation requirements see Articles 1180 and 769.h.1.

(2) Accountability. The SKL is a ALC 1 item and must be continuously accounted for as discussed below.

(3) Safeguarding. With the CIK inserted and a user logged on to the device, the SKL must be handled and safeguarded at the highest classification of key stored in the device.

(4) Inventory requirements. In a watch environment, the device and associated CIK will be accounted for on a watch-to-watch inventory. In a non-watch environment, the device and CIK shall be accounted for by sighting such against the local custody document. See Article 1181 for inventory requirements for electronic key.

(5) Destruction. There is no requirement to physically document destruction of key in a SKL. SKL Audit Trail reviews will serve to verify deletion/destruction of key.

NOTE: Providing these reviews are accomplished and documented in an Audit Trail review log the need for paper destruction records and wet signatures is not

required. Audit Trail reviews, including the frequency of them and by whom they are to be conducted should be clearly addressed in the accounts Local Handling Instruction and any Letters of Agreement for support to Local Element (LE) personnel accountable to a CO other than that in which the device/material is charged to.

(6) The loss of Traditional or Modern Key as a result of a device failure or database corruption must be reported to the supporting Account Manager as discussed in paragraph 8 to Annex AE.

9. Audit requirements:

a. The SKL automatically records keymat movement by *individual* users and can record a sizeable audit trail of up to 2 MB. The LMD however has a 32 KB limit and although LCMS 5.1.X will allow for uploads via the LMD directly (not the KP) up to the 2 MB limit, uploading a file of that size over the serial port has been clocked at 20 hours in a laboratory/test environment – not a very feasible option. SKL programmers have responded by devising a temporary workaround in the form of a warning banner screen. It displays on the SKL when the audit trail is at some point below the 32 KB limit, reminding the SKL operator that the audit information must be uploaded. Other feasible alternatives are reviewing the audit trail manually (on the device itself) or uploading the SKL audit trail to another computer workstation running Data Management Device Power Station software (DMD PS). The latter supports uploading the SKL audit trail in chunks for a total upload time of about 20 to 30 minutes.

b. Audit data must be reviewed at a minimum of monthly or more frequently, as required by the SSO, EKMS Manager(s) or LE Issuing that issued the keymat or by a person specifically designated in writing by the local command to conduct the reviews. It is **HIGHLY** recommended that Audit trail data be reviewed NLT the 5th working day of the month following the month in which the material was issued.

c. Except as indicated in note 3 below, failure to review audit trail data for equipment with audit capability (e.g. DTD, SKL, TKL) **when initialized and/or storing key or are issued to a LE** within the prescribed time frames will be reported as a COMSEC Incident in accordance with Article 945. Documentation/Retention requirements will be in accordance with

Annex T.

NOTES: (1) The 5th working day of the month following the month in which the material was issued is HIGHLY recommended as the material issued to the Local Elements which is superseded will not only be reflected on the LE Working Destruction Report from LCMS but must also be reflected on the accounts Consolidated Destruction Report which must be dated NLT the 5th working day of the month following supersession. Key reflected on a signed destruction report as destroyed found to still exist must be reported in accordance with Art 945.e.

(2) In instances where a device is issued on an irregular basis (FLT CINC Communicator), exercise, middle of the month, etc… and the device will not be returned to the EKMS Manager for review, the audit trail will be reviewed by either a properly cleared and authorized Supervisory user for the LE activity and recorded in an Audit Review Log (if issued for 30 days or longer) or by the EKMS Manager upon turn-in, whichever occurs sooner.

AMD-9

(3) Reviews of DTD, SKL, or TKL audit trail data for devices issued to ~~CMS A&A~~ COR Audit Teams or school houses where the EKMS Manager Course of Instruction (COI) is facilitated are not required unless such is mandated as a matter of local policy by the supporting EKMS account or in ISIC and/or TYCOM directives. Devices used by these entities are restricted in purpose to training functions and is limited to either Test Key or ALC 7 material produced from a non-operational Key Processor (TESTPAC).

d. Reviews may be accomplished using any of the methods outlined in paragraph 9.a. above. The reviewer must be someone other than an authorized User of the SKL and must be familiar with the operational use of the particular SKL.

AMD-9

e. Audit reviews **must be** documented in an Audit Data Review Log and the log retained in accordance with Annex T. A sample log for both reinitialization and Audit Trail reviews can be found on the NCMS CAS portal. Logs are subject to inspection/review by the supporting COMSEC Account, ISICs/IUCs and ~~CMS Advice and Assistance~~ COR Audit Teams. [**NOTE**: It is important that SKL Users understand that the audit trail, even when full, will not interfere with SKL operation and will overwrite the oldest audit entries.]

f. The following SKL audit records will be reviewed at a minimum for anomalies (e.g., operator activity at unusual times, excessive transfers of key or fills, improper upload or maintenance of audit data, etc.):

(1) Alarm event entry

(2) Audit trail full

(3) Audit trail initialization

(4) Audit upload

(5) CIK initialized

(6) Connection to a device

(7) Data or stored key

(8) Date change

(9) Information/Data transfers

(10) Key file received

(11) Key file transferred

(12) Key received

(13) Key transmitted

(14) Key zeroized (destroyed)

(15) KOV 21 zeroized

(16) Login/Login failure attempts

(17) Time change

g. Providing reviews are free of anomalies, the EKMS Manager(s) or other designee(s) may delete the data from the computer (to which it was uploaded) or from the SKL. Anomalous data must be preserved in support of local and/or external (e.g., NCIS) investigation and must also be classified a minimum of Confidential pending investigation and resolution.

10. **Shipping**:

a. When the SKL contains keymat but the initialized/associated CIK is removed and no classified data is stored on the host side, ship in accordance with Article 535 herein.

b. Ship the initialized/associated CIK separately from the SKL so as not to have them arrive at the same time/in the same shipment. Except where paragraph 10.c. applies, report non-compliance with this restriction as a COMSEC incident in accordance with Article 945.

c. In the case of an operational emergency (local, on-scene commander directs shipment of the SKL and its initialized/associated CIK together), ship using the methods approved in this manual for highest classification of keymat or host side data in the SKL.

11. **Data Transfer and Effect on Classification of SKL and Computer**:

a. Downloads:

(1) Downloads of unclassified software or unclassified data to the SKL from a classified computer: No change to current classification of SKL or computer.

Note: With the concurrence of the IAM and/or DAA a SKL which is not storing either keying material or classified data may be connected to either a standalone or networked computer via the fill port to download unclassified software or data from an approved source. This latitude is strictly limited to the use of an empty SKL. The connection of a device storing either keying material or classified data must be reported as a security violation or spillage, as applicable.

(2) Downloads of classified data (non-keymat) to the SKL: Change; SKL becomes classified to at least the level of the downloaded data.

(3) Downloads of classified data to the SKL may be no higher than Secret. Failure to comply with this restriction is a reportable COMSEC material incident. (The SKL can store keymat of all classification levels and categories that has been Type-1 encrypted.)

b. Uploads:

(1) Uploads of unclassified data, encrypted keymat, or other unclassified material to a computer: No change to current classification of the SKL or computer. Neither will this action necessitate or impose a handling designation/caveat for the computer. This includes when the SKL is unclassified and the computer is classified.

(2) Uploads of data from the SKL to a computer having a higher classification than the SKL: No change to the current classification of the SKL or the computer.

12. <u>Procedures for Failed SKL Devices</u>:

a. When zeroization feature/function fails on SKL:

(1) Remove the batteries and the CIK and handle the SKL as classified. Store the SKL and its associated CIK apart from each other (in separate security containers).

(2) Promptly notify NCMS N3 by naval message and request disposition instructions (where to turn in device for repair).

b. When SKL fails “out of the box” or while in operational use: Promptly notify NCMS N3 and request disposition instructions.

c. Protect failed SKL devices to the highest level of keymat or data they contain at time of failure.

Note: To minimize damage to the SKL fill ports and enhance the lifespan of the device, prior to issue and periodically, as warranted it is recommended that a small amount of silicone gel be applied to the fill port. The gel is available in via supply channels under the National Stock Number (NSN) 6850-00-177-5094. Ensure compliance with applicable safety procedures including the Material Safety Data Sheet (MSDS) in handling, using or storing the product.

13. Assess risk to Determine Adequacy of Security Measures:

a. Factors that must be weighed to determine risk posed to SKL:

(1) Classification and quantity of key

(2) Classification and sensitivity of information protected by key

(3) Cryptoperiod length and net size

(4) Threat environment

(5) Access to the key

(6) Sensitivity of information on host side

(7) Life span of information protected by the key (strategic/long-term or tactical/short-term)

b. Depending on the level of risk, these added security measures can be taken (assumes minimum security measures will be met, too).

NOTE: Each successive grouping of security measures is cumulative (each includes those previously listed):

(1) Low risk: Adhere to minimum security measures of this interim doctrine.

(2) Medium risk: Store SKL and/or initialized/associated CIK in a GSA-approved security container. If individuals other than bona fide SKL users have access to the security container, store the SKL and CIK in separate containers.

(3) High risk: Classify and handle the SKL to the highest level of keymat or host side classification whether the initialized/associated CIK is inserted or not.

(4) Very high risk: Implement TPI procedures (handling and storage) to SKL devices storing Top Secret Key (Type-1 encrypted) or to the initialized/associated CIK.

c. To lower risk and the attendant need for added security measures, commands should reduce keymat stored in each SKL to the absolute necessary for operations. Another means of lowering risk is to super-encrypt keymat prior to storage in the SKL.

14. Emergency Actions: In the event of impending site overrun and/or capture, zeroize the SKL. Then, as time permits, destroy the SKL beyond use as well as its embedded KOV 21 cryptographic card (smash with a fire axe, hammer, or other heavy object).

15. Reportable COMSEC Incidents Unique to the SKL: The Incidents reflected below are device specific and supplement those reflected in Chapter 9. Local Elements/Users must promptly report the occurrences below to the SSO/EKMS Manager for further reporting.

a. Reportable COMSEC Incidents:

(1) Lost/stolen SKL.

(2) Loss of initialized CIK, when the associated SKL was not in continuous protective custody or securely stored.

Note: If a CIK is lost and the SKL has not been outside of proper storage or the direct control of an authorized user, promptly delete the lost CIK from its associated SKL, report it to the SSO, LE Issuing or EKMS Manager, as applicable and document it locally as a non-reportable PDS.

(3) Failure to delete a lost/stolen CIK from its associated SKL.

(4) Unauthorized and simultaneous access to a SKL and its initialized/associated CIK.

(5) Use of a SKL device with a breach or other evidence of tampering in its casing/housing.

(6) SKL serial number not the same one as recorded on inventory and it is clear that the serial number on the inventory was not entered erroneously (e.g., one or more numbers transposed).

(7) SKL used to transfer unencrypted (red) keymat via STE with non-approved adaptor/connector cable.

(8) SKL and initialized/associated CIK found outside of required protective custody.

(9) Failure to ship the initialized/associated CIK separately from the SKL, or failure to stagger shipment of SKL and initialized/associated CIK to avoid having them arrive at the same location at the same time.

(10) CIK update count is higher in the SKL than on the CIK (possible evidence of unauthorized copy)

(11) Key is loaded on host side by means of a data/program load, but should only be loaded on the host side using "command request".

(12) Unauthorized cryptoperiod extensions of LKEK and HDPK. (SKLs in-use must be reinitialized annually when used to store/protect key). This is not applicable to devices which have not been initialized (in the box or stored at the Managers level and not protecting key)

(13) Failure to review and/or document reviews of audit data (except as indicated in paragraph 9.c (Note 3) above).

(14) Discovery of a breach or tampering in the SKL casing/housing.

(15) Opening or tampering with the KOV 21 cryptographic card housing by anyone other than the depot or manufacturer.

(16) Downloads of classified data exceeding the Secret-high level.

NOTE: Placement of classified data in the SKL is restricted to the Secret level.

16. <u>Taking SKL Device out of Use/Service</u>: Before being taken out of use, the existing audit trail must be uploaded and deleted from the SKL. The SKL will then be zeroized to delete all data on the host side, as well as to destroy all keymat associations with initialized CIKs. However, this action will not delete SKL operating software, UAS, or new audit trail information. Zeroizations will only delete information located in working memory and storage memory (the encrypted database). The SKL can then be taken out of service and used at a later time.

17. **Guidance Unique to Depot (e.g., Crypto Repair Facility, COMSEC Material Issuing Office/CMIO) or Manufacturer levels only**:

a. KOV 21 Accountability:

(1) Although the KOV 21 is transparent to the end user, it must be continuously accounted for by serial number/controlled as an ALC 1 item per EKMS 1 (series). An off-line inventory at the depot must be maintained that readily identifies into which SKL casing a particular KOV 21 has been embedded.

(2) Beyond the depot/manufacturer level, the KOV 21 is not accountable (separately from the SKL).

(3) In the event of a depot COMSEC Account audit, the off-line inventory will replace the mandatory sighting of the embedded KOV 21.

(4) The KOV 21 card shall only be removed at an authorized COMSEC service depot location, when necessary, to repair or replace the card. Opening or tampering with the KOV 21 housing by anyone other than the depot or manufacturer is a COMSEC Incident that requires reporting per EKMS 1 (series).

b. Screw head coating (epoxy) control requirements: This coating supports tamper detection on the SKL. Contact NCMS N5 for this national-level guidance, as needed.

c. Some SKLs have been discovered to have loose fill connectors. Units with defective SKLs must request disposition instructions from NCMS in accordance with EKMS-5(series).

18. **Operating training**:

a. To request SKL operator training, contact SPAWAR Systems Center Charleston (SCC) point of contact Ms. Scarlette Reid at commercial (843) 218-4489.

ANNEX AG

LCMS SYSTEM FAILURE and RECOVERY PROCEDURES

1. The procedures contained herein will be adhered to in the event of a failure of the LMD, the associated hard drive or the KOK-22 (KP).

a. **Background:** The loss of either the Local Management Device (LMD) and/or associated KOK-22 (Key processor) will result in the account having to revert to manual SF-153s (for issuing either equipment or physical material, or electronic key outside LCMS (if available from a host DTD or loaded from canister-packaged material, if available). Additionally impacted will be the loss of the ability to order, download and issue electronic key pending restoration of the system.

b. **Minimizing the impact of a catastrophic failure:** EKMS Managers must perform periodic clean-up and maintenance procedures discussed in Article 718 and Annex X as outlined in EKMS-704(series).

c. **Replacement units or equipment:** EKMS-5(series) contains procedures to request both replacement KOK-22As and disposition instructions. Additionally, these accounts, as well as servicing ~~CMS A&A Training~~ COR Audit Teams possess spare hard drives, should an account require a replacement drive pending receipt of a new drive from the EKMS Help Desk.

AMD-9

d. **Pre-requisites to minimize the impact of a failed hard drive or KOK-22 failure:**

1. EKMS Managers **MUST**;

a. ensure at least two personnel are registered in LCMS with a KP account (if equipped with a KOK-22) and that both know their password and/or pin or have them properly stored and accessible.

b. know what the current root password is. You **cannot** perform database maintenance or restores without it.

c. conduct archives and back-ups as outlined in EKMS-1(Series) or more frequently, as required.

d. maintain an up-to-date print-out of their Accountable Item Summary (AIS) and Transaction Status Log (TN

Log). This **cannot be over-emphasized** in the event an account has to manually re-create their AIS due to corruption of the backup media or from the point of the last backup if not performed in accordance with the frequency outlined in this manual.

e. have an up-to-date backup tape (for hard drive failures) and/or the current REINIT 1 and NAVREINIT 2 CIKS.

NOTES: (1) Failure to understand the importance of performing the items above in paragraph (a) WILL result in the expenditure of numerous man hours, the potential loss of accountability of material and the need to request replacement material for material received after the date of the last LCMS backup held by the account.

(2) If a restore is performed, a 2nd LMD Operator with a KP account is required. When log-on is attempted, this will force the KP to indicate "KP List Rollback" requiring two personnel.

2. Actions to take in the event of a failure of the LMD and/or KOK-22 (KP):

1. Document any error codes displayed or symptoms observed that may be helpful in expediting resolution of the matter.

2. Contact the EKMS Technical Support Center at 1-877-NAV-EKMS (628-3567).

3. If the EKMS Technical Support Center is not able to resolve the matter or it is determined that the LMD, removable hard drive, or KP require replacement or the failure is 07 days or longer in duration, the failure will be reported via official message by the unit experiencing the failure no later than the next working day following the 07 days to the organizations noted below. Failure to report outages greater than 07 days in duration will be documented as a non-reportable PDS.

NOTE: In addition to other required addees, ensure CMIO Norfolk VA, NCMS Washington DC, SPAWARSYSCEN Atlantic Charleston SC and the Strike Group or ESG Commander, as applicable are included in the message. (The inclusion of the Strike Group or ESG Commander is for afloat units only to facilitate replacement of faulty equipment, when deployed). See paragraph 1.c above for further guidance.

4. Following notification via naval message, NCMS will mark the account as "suspended" thereby stopping all shipments of material from the Central Facility, Tier 1, or CMIO Norfolk until the account is restored and new FIREFLY Credentials have been posted. Immediately upon restoration of the account and successful posting and verification of new FIREFLY Credentials, the unit **MUST** notify NCMS by naval message in order to remove the "suspended" flag.

> **NOTE: It is imperative once the account is marked as "suspended" the account not connect to the message server and retrieve and process the accounts CAD data. Doing so will prevent the account from performing local custody issues and prohibit the ability to submit necessary accounting transactions for system restoration and hinder resupply actions.**

a. **<u>KOK-22 (KP) Failure</u>**: (In addition to 2.1 – 2.3 above)

1. The account experiencing the failure will submit a Naval message to NCMS requesting disposition instructions for the failed unit. Cite any phone conversations, emails, or other correspondence with the EKMS Technical Support Center in the message.

2. NCMS will provide disposition instructions for the failed unit and will also direct, the transfer and shipment of a replacement KOK-22 and the associated Transit CIK.

3. Upon receipt of the KOK-22 (KP), the receiving account will; report receipt of the replacement unit and the Transit CIK, as well as prepare the transfer documentation, package and ship the failed unit via DCS channels.

> **NOTE: Transit CIKS will not be shipped with the associated KP. They may however be packaged together and transported if cleared command personnel are used as couriers.**

4. The receiving account will follow the procedures outlined in the EKMS-704 (series) (Reinitialize KP, Chapter 9) to bring the replacement KOK-22 (KP) online.

b. **<u>LMD Failure or Failed Hard Drive</u>**: (In addition to 2.1 – 2.3 above)

1. If it is determined by the EKMS Technical Support

AMD-9

Center that the hard drive is faulty, a replacement drive can be obtained by contacting the local ~~CMS A&A~~ COR Audit Team or from either the Strike Group or ARG Commander for afloat units which are deployed, as applicable.

> **NOTE: Drives associated with the LMD are not COMSEC accountable but are classified SECRET. Accordingly, LMD hard drives must be shipped via authorized methods with a Record of Receipt (OPNAV 5511/10) enclosed with the shipment as discussed in SECNAV M5510-36 (Series) 9-10.2.**

2. Once the replacement drive is installed, the EKMS Manager will have to perform a restore of the LCMS database as outlined in the EKMS-704 (series) Appendix F.

3. Conduct a "Change of Account Location" (COAL) inventory. The COAL is recommended instead of a Semi-Annual Inventory Report (SAIR) in order to prevent affecting the account's assigned fixed-cycle inventory month.

4. If the latest backup media is over 7 calendar days old or any transactions were performed after the last backup, conduct a complete inventory of all material held/charged to the account, including electronic key material. If no transactions have been performed since the last backup and the backup is within 7 calendar days, a physical inventory is not required but step (5) below will be conducted.

5. Print and compare all entries reflected on the Accountable Item Summary against the most recent Inventory Report from the Central Office of Records (COR).

6. Coordinate with the COR to report/resolve any inventory discrepancies.

> **NOTE: As stated above, following the restore, the initial log-on to the KP will require a second operator to log-on to re-bind the LMD/KP (This is referred to as a KP List Rollback).**

(2) Any transactions performed in LCMS after the date/time of the backup MUST be performed again to ensure the Accountable Items Summary and Transaction Log accurately reflect the material status and location of all items.

(3) Any modern key ordered/received, credentials exchanged/downloaded, or electronic key received via: Direct

COMMS, the X.400 message server, etc... **must be** requested if they were received after the date/time of the last backup as discussed in paragraph 3 below.

(4) If the EKMS Manager has an up-to-date print out of the AIS and TN log and performs database maintenance as required, the impact of a system failure is greatly lessened in terms of duration and level of effort required to restore the system.

(5) To effect timely delivery of replacement material if required, contact NCMS Operations Department (N3) and CMIO Norfolk.

3. **Replacement of Electronic Key due to LMD and/or KP Failure:**

(1) If the failure of a LMD and/or KP results in the loss of electronic COMSEC keying material that can not be recovered, the EKMS Manager must follow the procedures outlined in this article to recover the destroyed electronic COMSEC keying material.

(2) The account must manually prepare and submit (via fax or email) an SF-153 destruction report to NCMS Washington DC listing all electronic COMSEC keying material destroyed due to the LCMS system failure. (If necessary, a hard copy SF-153 can be downloaded from the NCMS CAS portal. See Annex S for the new URL). The destruction report must clearly state that the report is being submitted due to a loss of electronic COMSEC keying material as a result of a LMD and/or KP failure. Accounts can use their most recent Accountable Items Summary (AIS) to determine the material that was destroyed as a result of the failure.

NOTE: Resupply actions cannot be initiated until the manual destruction report is submitted to, received by, and processed by NCMS.

(3) If the account holds mission critical electronic COMSEC keying material that must be resupplied to the account prior to restoration of the LMD and/or KP, the EKMS Manager must send a message to; NCMS, the Controlling Authority for the material, CMIO, and DIRNSA identifying the Short Title(s) and Editions of material required as well as the preferred method of delivery (e.g., STE to STE transfer, OTAT/OTAR from command in area, or issue of key from another account in the area).

(4) Upon restoration of the LMD and/or KP, preparation, submission and processing by NCMS of the manual SF-153 destruction report, the account must send a message requesting resupply of all electronic key inadvertently destroyed due to the system failure:

```
TO:   Controlling Authority (list each individually)
      NCMS WASHINGTON DC
      CMIO NORFOLK VA
      DIRNSA FT GEORGE G MEADE MD
CC:   ISIC
      CHAIN OF COMMAND
MSGID/GENADMIN/USS NEVERSAIL/-/-//
SUBJ/RESUPPLY OF ELECTRONIC COMSEC KEYING
MATERIAL DUE TO A LMD AND/OR KP FAILURE//
REF/A/DOC/NCMS WASH DC/-//
AMPN/REF A IS EKMS-1(SERIES)//
POC/U.B. UNDERWAY/CVN72/EKMS MGR/PRI:619-553-
4290/EMAIL:UNDERWAY(AT)CVN72.NAVY.SMIL.MIL//
RMKS/1. IAW REF A, REQUEST RESUPPLY OF THE BELOW
REFLECTED SHORT TITLES DUE TO A LCMS SYSTEM FAILURE:

   A.  ACCOUNT NAME / ACCOUNT NUMBER:
   B.  EKMS TECHNICAL SUPPORT CENTER TROUBLE TICKET
       NUMBER:
   C.  HARD COPY DESTRUCTION REPORT SUBMITTED TO NCMS
       YES / NO
   D.  CONAUTH / SHORT TITLES REQUESTED FOR RESUPPLY:
       1. JCMO:
          USKAD XXXXXX
          AKAD XXXXX
         (INCLUDE CENTRIX SHORT TITLES IF APPLICABLE)
       2. COMUSFLTFORCOM:
          USKAD XXXXX
          AKAD XXXXX
   E.  REMARKS:
```

NOTE: A list of electronic short titles can be obtained from either the accounts most recent Accountable Item Summary (AIS) or most recent Status of COMSEC Material Report (SCMR). Contact NCMS if additional assistance is required in completing the list of short titles which may be required.

(5) User Representatives must submit new key orders to the EKMS Central Facility for replacement of modern or enhanced FIREFLY key recovery.

ANNEX AH

COMSEC Management Workstation (CMWS)/Data Management Device Power Station (DMD/PS)

1. **Purpose and applicability**:

This annex is intended to provide guidance to Department of Navy (DON) EKMS Managers and LE personnel in the use, safeguarding and management of the DMD PS User Application Software (UAS) Version 5.0.4 or 7.0.

2. **DMD PS Description/Use**:

a. DMD PS is a Windows-based application intended to support Tier 3/Local Element (LE) personnel in the management of Common Tier 3 (CT-3) payload data and encrypted (black) keying material (keymat).

b. CT-3 uses the concept of a payload hierarchy comprised of a culmination of; Platforms, Equipments, Key Tags, and Keys which make up a payload to manage information and support equipment-based key and data distribution. At the top of the hierarchy is the Package (if used), then the Platform (e.g., CVG), followed by one or more Equipments that have fill locations. Both Key Editions and Key Segments (including key tags) are located at the bottom of the hierarchy.

NOTE: Devices such as the AN/CYZ-10(V3) running CT-3 User Application Software (UAS), Simple Key Loader (SKL), ~~and~~ the Secure Data Transfer Device 2000 System (SDS) and Tactical Key Loader are referred to as Modern Fill Devices (MFDs).

c. DMD PS can be deployed on either a desktop or laptop computer herein referred to as the Tier 3 COMSEC Management Work Station (CMWS). Minimum system requirements are reflected below:

(1) Windows 7 (Operating System)
(2) Data Management Device (DMD) Power Station (Version DMD PS 5.0.4 (XP) or 7.0 (Win 7.0)
(3) Internet Explorer 10 ~~5.5~~ or higher
(4) DTD Audit Utility (Version 1.0 or higher)

d. In combination with the Tier 3 CMWS, the DMD PS UAS is a very powerful COMSEC management tool used by either Local Elements (LEs) or EKMS Managers to; receive, store, issue, and destroy electronic encrypted (black) keymat and track physical COMSEC material as well as generate all required accounting reports (SF-153s). The use of the CMWS enables cryptosystem-specific payload data and its associated encrypted keymat to be issued to a fill device for immediate use in End Cryptographic Units (ECUs). All CMWS fielded with the CMWS/DMD PS UAS by SPAWAR will be STIG-hardened and configured to operate on a standalone computer.

e. Although MFDs afford the ability of creating and managing CT-3 payload data for equipment-based keymat distribution, such functions, when performed on MFDs are manually intensive, error prone, and possibly reduce battery life. DMD PS has a more intuitive user interface to support the creation and management of CT-3 payload data as well as the assignment of imported encrypted keys to the CT-3 payload. When used for Tier 3 management functions, the DMD PS offers improved performance and functionality than a MFD by itself and also permits longer storage/reuse of the CT-3 payload data.

f. The DMD PS can manage *encrypted* key only (Transfer Key Encryption Key (TrKEK)-wrapped or End Crypto Unit (ECU) KEK-wrapped). It is critical that unencrypted (red) key material (keymat) **not** be loaded on the DMD PS. The loading of red (unencrypted) key on a CMWS/DMD PS is a COMSEC Incident.

g. To prevent the inadvertent loading of unencrypted key into the CMWS/DMD PS, the **only** authorized distribution paths for loading encrypted keys into the Tier 3 CMWS will be restricted to devices or connections identified below:

(1) Via removable floppy disk or CD media that was produced on a LMD/KP using CUAS or

(2) Via the LMD STE with the CMWS set up in LCMS as a STE Local Element, when approved. (**See note below**)

NOTE: The Tier 3 CMWS receives TrKEK encrypted key from the LMD/KP via removable floppy or CD media. The CMWS is not permitted to connect directly or via STE to the LMD/KP. Over-The-Air-Distribution (OTAD) is authorized between two CMWSs connected via STE.

h. CMWS/DMD PS supports equipment-based keymat distribution through enabling the development of a CT-3 payload on a computer, enabling the importation and storage of encrypted keymat received and distributing CT-3 payload and/or encrypted keymat to the fill device. The DMD PS supports the creation of a CT-3 payload for both *key needed* and *database receive* modes of the fill device, as well as supports the local management of issued COMSEC equipment/physical assets. The CMWS/DMD PS can create and manage the following types of CT-3 payload(s): Platforms, Equipments, Key Tags, and Signal Operating Instructions (SOIs). The CMWS/DMD PS can also import XML-formatted encrypted keymat via media originating from CUAS and support the importation of other media formats for legacy ECUs (e.g., JTIDS floppy format). Received encrypted keys can either be DTD-TrKEK encrypted or ECU-KEK encrypted. The key attributes displayed for the received keys also indicate the decrypting KEK type along with the decrypting key’s attributes.

NOTE: Paragraph 3.d of this document identifies the only external source devices that may be used to import encrypted keymat.

i. After creation on the DMD PS, the databases containing the CT-3 payload (for both *key needed* and *database receive* modes) can be downloaded to a MFD. For *key needed* mode: once the payload has been downloaded, the keymat may be loaded in the MFD from the corresponding key source specified in the payload. For *database receive* mode: the encrypted keymat can be downloaded with the payload into the MFD. The CMWS/DMD PS contains fill locations for all common ECUs. Accordingly, the keymat is automatically assigned to its key locations as determined by the downloaded payload.

j. Dependent upon the function intended by the operator, the CT-3 payload hierarchy concept can be applied in different ways within the CMWS/DMD PS. The CMWS can contain one or more platforms. The User may define an airplane, ship, tactical vehicle, or radio as a platform consisting of one or more pieces of equipment. How the User defines the platform depends on how many pieces of equipment the User is managing, the operational environment, and/or the operations the User is trying to accomplish. Two examples of hierarchies are as follow:

(1) An aircraft carrier maintains an F14 aircraft. The F14 contains cryptographic equipment (radio). The radio contains fill locations for keys and Transmission Security (TRANSEC) data. The F14 is defined as a platform. The

cryptographic radio is defined as equipment and the CMWS/DMD PS has the appropriate fill locations for that equipment type.

(2) A tactical vehicle contains cryptographic equipment (radio). The equipment contains keys and TRANSEC data. The tactical vehicle is defined as a platform. The equipment (radio) is defined as equipment and the DMD PS has the appropriate fill locations for that equipment type.

k. CMWS/DMD PS supports the following:

(1) Assignment and management of segment effective dates.

(2) Setting up account packages, containers, devices, and Users.

(3) Local custody issue, physical inventorying, destruction of COMSEC keymat and generation and printing of required documentation (SF 153s).

(4) Displaying and printing both previous reports and blank forms (working copies).

(5) Backup and restoration of the DMD PS database/platform template. A platform template can be maintained on the CMWS/DMD PS.

AMD-9

NOTE: To protect against the irretrievable loss of data in the event of CMWS/DMD PS failure, system backups (on removable storage media) must be performed at a minimum of monthly although system usage or local policy may dictate a greater frequency. Failure to perform backups at a minimum of monthly is a non-reportable PDS in accordance with Chapter 10. Compliance is subject to review during formal ~~ISIC inspections and CMS Advice and Assistance Team visits~~ COR Audits.

3. **Maximum Level of Operation/Use**:

a. The CMWS/DMD PS is not; COMSEC Accountable (CCI), assigned an Accountability Legend Code (ALC) or accountable within the COMSEC Material Control System (CMCS).

b. The CMWS/DMD PS is designed to receive, store, manage, and distribute (issue) electronic encrypted (black) keymat. It does not have the ability to either; generate, encrypt, or store unencrypted (red) keymat. Unencrypted keymat (red) must **never** be introduced into the Tier 3 CMWS/DMD PS. The introduction of unencrypted (red) keymat into the CMWS/DMD PS **must be** reported as a COMSEC Incident.

c. National policy dictates that the Tier 3 CMWS hard drive be classified, operated, stored, controlled, shipped and safeguarded at the Secret level. This does **not** imply unencrypted (red) keying material classified Secret or below can be loaded or introduced into the CMWS/DMD PS. Information technology interface flow rules coupled with the association of cryptographic keys that are originated from the account's classified LMD/KP require that the system and related components be protected at the Secret level. Additionally, it is anticipated that COMSEC-related data originating from the Local Management Device (LMD) will be routinely uploaded to the Tier 3 CMWS/DMD PS via the methods approved in paragraph 2.g. Unauthorized access or the physical loss of a Tier 3 CMWS/DMD PS or its associated hard drive must be reported as a COMSEC Incident.

d. In accordance with the 26 March 2012 Approval to Operate (ATO), connection of a STE to the CMWS/DMD PS is authorized. The CMWS may also be connected to an external printer via serial port or NSA-approved fill devices, i.e. DTD, SKL, and TKL. **Connections between the CMWS/DMD PS and any device not specifically authorized herein, including either an internal or external network regardless of classification must be reported as a COMSEC Incident.**

e. Removable storage media extracted from the Secret-high CMWS must be handled, labeled, stored and safeguarded at the Secret level. Secret removable media containing encrypted (black) keymat may be declassified using local command-approved procedures (e.g., degauss or overwrite) and reused for the **same purpose** or the media may be destroyed using approved destruction procedures for its classification.

f. To ensure the availability, integrity, and confidentiality of the approved and accredited CMWS/DMD PS platform, the CMWS/DMD PS will be **dedicated** to Tier 3 CMWS/DMD PS operations only.

NOTE: DMD PS User passwords will be classified, safeguarded and controlled at the Secret level. Individual access controls (permissions) should be

implemented, tested and documented to restrict access to the DMD PS database and encrypted key when space limitations result in the DMD PS hosting other applications used by personnel not performing COMSEC related functions on the DMD PS.

g. The CMWS/DMD PS is not required to be TEMPEST certified however, operating locations/environments will dictate the need for facility TEMPEST countermeasures.

h. Though the DMD PS software is available through other sources, the Navy In Service Engineering agent (ISEA) is the only source responsible and authorized for fielding of the CMWS/DMD PS within DON. Changes or modification to the configuration settings of the CMWS/DMD PS UAS **are not** authorized and may invalidate the system accreditation.

4. **Personnel/Access Control/Physical Security Requirements**:

a. The IAO/IAM, EKMS Manager or other properly cleared, trained, mature and responsible individual designated by the local commander as applicable must oversee the integrity of information in the CMWS/DMD PS. The IAO/M or EKMS Manager as determined by local policy will grant User access to properly cleared individuals whose official duties require access to the Tier 3 CMWS/DMD PS. Such access will either be in the form of an individual designation letter or access list for the space in which the CMWS/DMD PS is installed/operated. If an access list is used to identify those authorized access to the CMWS/DMD PS, it is recommended that notes or legend codes be used to distinguish such personnel. If used, access lists will be updated in accordance with article 505.

AMD-9

b. It is highly recommended CMWS users receive local CMWS User Familiarization Training prior to deployment or operation of CMWS. Potential sources for CMWS User Familiarization Training include EKMS Account Managers/Users who have experience with CMWS, Contractor Support Personnel, ~~COMSEC Advice and Assistance (CMS A&A)~~ COR Audit Teams, I MEF (Camp Pendleton, CA), II MEF (Camp Lejeune, NC), III MEF (Okinawa, Japan), and Space and Naval Warfare Systems Center Atlantic.

c. A valid userid and password is required to logon to the Tier 3 CMWS/DMD PS.

d. Users should limit the amount of time they are logged-on to the CMWS/DMD PS to that which is required to perform official job functions and must completely log-out of the Tier 3 CMWS after completing job functions.

e. Leaving a DMD PS logged on and unattended or the loss of either a CMWS/DMD PS or its associated hard drive must be reported as discussed in paragraph 3.c. as a Physical COMSEC Incident.

5. **User Password/Account Management**:

a. Access to the CMWS/DMD PS is restricted to properly cleared and authorized personnel and is enforced through individual user accounts and a valid password.

b. Authorized users of the CMWS/DMD PS will have an individual userid/password. The sharing of passwords and use of either generic accounts or group accounts is **prohibited**.

c. Activities with a CMWS/DMD PS installed and in-use will designate a properly cleared and trained individual meeting, at a minimum the same grade requirements as a LE Issuing, to be the System Administrator (SA) for the CMWS/DMD PS. Unless prohibited by local, TYCOM or higher policy, the EKMS Manager, Alternate or Tier 3 LE Issuing/Alternate, may also have access to/perform the duties of the SA. Only functions which require administrative rights (i.e. software upgrades, access to Security logs, creation of or unlocking of accounts, etc., shall be performed under the local administrator account. Regular use and day-to-day functions performed on the CMWS/DMD PS will be performed by authorized personnel under their own individual user account and password.

All other accounts must be set up as a “user” on the workstation or laptop, as applicable.

d. The sharing of passwords is not authorized and **must be** reported as a COMSEC Incident.

e. Passwords must be comprised of a minimum of 14 characters to include: two upper-case, two lower-case, two numeric, and one special character consistent with good security practices reflected in the Department of Defense (DoD) Password Management Guideline, CSC-STD-002-85 or in SECNAV M-5239.1.

f. Consistent with DON EKMS policy for the Local Management Device (LMD), passwords must be changed at a minimum of every 90 days. More frequent changes may be dictated by either Local Policy or if compromise of a password is suspected or known to have occurred. **Should a password be compromised, the matter must be reported as a COMSEC Incident**, the associated user account should be disabled and access to the CMWS/DMD PS restricted until the Security Event Log can be obtained and reviewed by the IAO/M or EKMS Manager, as applicable.

g. Lockout parameters are configured to lock out the user account following three unsuccessful logon attempts. Should such occur the user account will have to be re-enabled by the designated System Administrator.

h. Passwords must not be written on or affixed to the Tier 3 CMWS/DMD PS. It is recommended that all Users record and appropriately safeguard their passwords on a SF-700 to prevent unauthorized access/use.

6. **Keymat Control Requirements Associated with CMWS/DMD PS Operation:**

Due to the strict prohibition of the introduction of unencrypted (red) keymat into the CMWS/DMD PS, only requirements related to the control and management of encrypted (black) keymat are addressed herein. Unencrypted (red) key will be handled, stored and safeguarded as discussed in Chapter 5.

a. Encrypted (black) keymat is defined as keymat that has been encrypted in a system approved by the National Security Agency (NSA) for key encryption. **Unless otherwise stated in the systems Security Doctrine,** when safeguarded and controlled *separately* from its associated Key Encryption Key (KEK) pending loading in an ECU or approved fill device, encrypted keymat is not considered CRYPTO but rather UNCLASSIFIED//FOUO. Absent such specific doctrine, equipment containing both encrypted keymat and its associated KEK are considered to hold unencrypted (red) key.

b. TPI handling and storage requirements are not applicable when encrypted keymat is safeguarded and controlled separately from its associated KEK.

c. Although encrypted key is considered UNCLASSIFIED//FOUO, media created on the CMWS is considered SECRET and must be labeled and safeguarded in accordance with

6.f below. To prevent a potential spillage or compromise of classified data associated information, except in a COMSEC emergency distribution will be restricted to SIPRNET only. Tracking, control, or accounting, will occur as though the data were sent in physical form.

NOTE: Direct connections between the CMWS/DMD PS and any device not authorized in paragraph 3.d is strictly prohibited and must be reported as a COMSEC Incident.

d. Although both the CMWS and LMD were exempted from CTO 10-25B requirements, this exemption does not extend to NMCI, One-Net or locally managed network clients subject to removable media policies. Managers desiring to send Black Key via SIPR must consult with their local IAM prior to doing so to ensure compliance with applicable IA regulations related to removable media including Computer Task Orders (CTOs), Naval Technical Directives (NTDs) and other IA regulations.

e. After initial receipt of a data package containing encrypted keymat, no further accounting for the original encrypted data package is necessary until the keymat in the package is decrypted. Once decrypted, the unencrypted (red) keymat is subject to the safeguarding, handling, and accounting requirements reflected in Chapter 5.

NOTE: Keymat that is decrypted (red) and exposed to human view/access must be accounted for within the CMCS. Keymat decrypted in a machine system from which unencrypted keymat cannot be extracted (e.g., benign fill equipment) does not require additional accounting.

f. Secret magnetic storage media containing encrypted keymat will be; labeled, accounted for, handled, safeguarded, stored and transported in accordance with Chapter 5. The media must be safeguarded and controlled at the Secret level and the notice "COMSEC ACCOUNTABLE" and a Short Title must be physically present on the media to indicate that the media requires tracking within the COMSEC Material Control System (CMCS).

g. With exception to keymat superseded through an emergency supersession in which the 12-hour destruction rule is applicable, routine destruction of encrypted (black) keymat is not subject to the 12-hour destruction rule set forth in article 540. Encrypted (black) keymat will be destroyed when no longer needed or upon routine supersession of the material, whichever occurs sooner.

h. Destruction of encrypted keymat that has an associated KEK may be accomplished by zeroization of all copies of the KEK. The zeroization process must include both overwrite of the keymat and zeroization of the KEK as soon as practical.

i. This document assumes the key’s unencrypted associated data (e.g., header or tagging information) is not sensitive. If not specified in the system Security Doctrine, the sensitivity of the associated data will be determined by NSA in conjunction with the material Controlling Authority (ConAuth). If either the header or tagging information is sensitive or requires additional security requirements, the ConAuth will advise accounts holding the material. If in doubt about the sensitivity or classification of an encrypted keymat’s associated data, contact the keymat ConAuth or NCMS N5 for assistance.

NOTE: Encrypted keymat may have classified or sensitive data (e.g., header or tagging information) associated with it. The associated data may or may not have been encrypted. If the associated data is not encrypted, the entire data package may be sensitive or classified (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.

j. Unless prohibited in the system Security Doctrine, there is no limit to the number of editions of encrypted keymat that can be issued to a User. This is contingent upon; (a) concurrence by the ConAuth and (b) the assumption that the Issuer (LE Issuing or EKMS Manager, as applicable) withholds the means to decrypt the keymat (the associated KEK) until a reasonable time before the effective period of the keymat with which it is associated.

7. **Audit Trail Review Tool and Review and Documentation Requirements**:

a. For the purpose of reviewing audit trail data, **only** the DTD Audit Utility Version 1.0 or higher is approved for use on the CMWS/DMD PS. Through the use of compression, there is virtually no size limitation for the audit trail. The CMWS/DMD PS can upload up-to the full 2 MBs of audit data which can be held by either the SKL or Secure Data Transfer Device 2000

System (SDS) at a faster rate than the LMD/KP which can only upload up-to 32 KBs of data.

b. MFD audit data must be reviewed at a minimum of **monthly** by the; EKMS Manager, Alternate, or LE Issuing that issued the keymat or other person specifically designated in writing by the local command to conduct the reviews. The reviewer **must be** someone other than an Authorized User of the particular MFD. Another alternative for uploading audit trail data for review is to do so manually on the device itself.

AMD-9

c. Audit trail reviews **must be** documented in an Audit Trail Review Log which is subject to review during either formal ~~ISIC inspections or CMS Advice and Assistance~~ COR Audit Team visits. In some instances despite the audit trail being full, operational use of the SKL may not inhibited however; the oldest audit entries will be overwritten. To ensure proper review of all functions performed since the last audit trail review, the frequency of use, amount of key stored in the MFD and local policy may dictate that reviews be conducted more frequently than stated above.

d. Minimum events to be reviewed when reviewing MDF audit data are reflected below. Some examples of anomalies include but are not limited to; operator activity at unusual times, excessive transfers of keymat, key received from an unknown source, improper upload or maintenance of audit data, etc.):

(1) Alarm event entry
(2) Audit trail full
(3) Audit trail initialization
(4) Audit upload
(5) CIK initialized
(6) Connection to a device
(7) Data or stored key
(8) Date change
(9) Information/Data transfers
(10) Key file received
(11) Key file transferred
(12) Key received
(13) Key transmitted
(14) Key zeroized (destroyed)
(15) MFD zeroized
(16) Login/Login failure attempts
(17) Time change

e. If no anomalies are detected, the audit trail data may be deleted from the Tier 3 CMWS (if uploaded) or from the MFD (if manually reviewed), as applicable. Audit trail data which reveals any anomalies must be classified at a minimum of Confidential and be retained pending local and/or any external investigation initiated.

8. **Procedures for a Failed CMWS**:

In the event of CMWS hard drive failure, LEs will promptly notify their supporting EKMS Account Manager who, in turn, will promptly notify NCMS N3 and/or the EKMS Help Desk and request disposition instructions and accounting guidance for both the failed hard drive and for the electronic keymat issued to and stored on the failed hard drive. The failed hard drive must be handled and safeguarded at the Secret level until properly sanitized or destroyed (using methods approved for Secret material).

9. **Security Compromise – Storage of Red Keymat on Tier 3 CMWS/DMD PS**:

The introduction or discovery of unencrypted (red) keymat in a Tier 3 CMWS/DMD PS, whether intentional or not **must be** reported as a COMSEC Incident via Naval message in accordance with Article 945. The initial incident report must request disposition instructions for the hard drive and any removable media used for back-ups. Additional actions required;

a. Until the unencrypted (red) keymat can be sanitized from the memory and the hard drive of the Tier 3 CMWS/DMD PS, the Tier 3 CMWS hard drive will be provided the same protection and accountability as required for the unencrypted (red) keymat being stored (i.e., stored~~aged~~ in a GSA approved container or vault and listed on the watch-to-watch inventory when at the LE level).

(1) If there is suspicion or proof of malicious activity (involving the hard drive and/or any removable storage media used as back-ups), the command reporting the incident must preserve and protect the hard drive and removable storage media "as is," pending local command or external (e.g., NCIS) investigation and/or NSA forensic examination.

(2) If it is clear that the storage of unencrypted (red) keymat was the result of a lack of familiarity with applicable security policy and/or training on the CMWS/DMD PS rather than willful intent to violate that policy, the Tier 3

CMWS/DMD PS hard drive and associated backup media will nonetheless need to be destroyed to ensure destruction of all unencrypted (red) keymat. See paragraph 10 of this document for approved destruction methods for hard drives and removable storage media used for back-up purposes. The destruction of the hard drive and associated removable storage media must be witnessed and documented on a local destruction record which will be retained with any related correspondence for two years. Additional destruction reporting or forwarding requirements will be defined by NCMS upon receipt of the incident report.

10. **Emergency Destruction/Actions**:

a. In the event of an impending site overrun and/or capture, the CMWS/DMD PS hard drive and any removable back-up media will be destroyed using any means available to prohibit the possible recovery of stored data (follow the local emergency action/destruction planning priority established for its current state of classification). If time allows (sufficient notification is given of possible site overrun or ordered withdrawal is to occur over a specified period of time, etc.), use the following destruction procedures:

11. **Information Assurance Requirements Related to the CMWS/DMD PS**:

a. Only software approved and provided by SSC Atlantic will be installed on the CMWS/DMD PS. For upgrades or new releases, SSC Atlantic will mail each account a self bootable image set which includes instructions for; archiving system audit files, exporting/importing the DMD PS database, applying the new image baseline and a "quick step" guide for the performance of routine CMWS operations.

b. Each image set is created for a specific CMWS hardware model. As a precaution, the account must confirm the Panasonic model number annotated on the face of the image set matches the model number found underneath the CMWS on the factory tag.

c. Upon receipt of installation materials, account managers must apply the mandatory image update set and report compliance via naval message to SSC Atlantic Code 58100. It is highly recommended any previous image sets and IAVA patches be destroyed upon successful installation of the new image set. **Only the new image set and future IAVA patches are to be retained for disaster recovery purposes.**

d. If operational requirements prevent compliance with the software upgrade by the established compliance date, the account must notify SSC Atlantic Code 58100 via naval message and specify a date in which the upgrade will be accomplished. Note: The image set media will become classified once placed into an operational CMWS and upon removal, should be labeled, stored and safeguarded at the SECRET level until destroyed.

e. EKMS managers or LE personnel responsible for management of the CMWS/DMD PS are required to update IAVM patches on a quarterly basis, or more frequently if notified by SSC Atlantic of a vulnerability requiring an immediate update.
Patches and instructions can be found at:
https://infosec.navy.mil/ekms/cmws.html

MATERIAL:	**DESTRUCTION METHODS:**	**PARTICLE SIZE REMARKS:**
Floppy disks	Degauss	
	"OR"	
	Burn	Crush ashes
	"OR"	
	Shred after removing jacket & metal hub	5 mm
Hard drive	Degauss	
	"OR"	
	Smelt	Temperature of 2800 degrees Fahrenheit required
Magnetic tape (digital & analog)	Degauss	
	"OR"	
	Burn	Crush ashes
Compact Disk (CD) **Digital Versatile Disk (DVD)**	Disintegrate	5 mm particle
	"OR"	
	Use optical media destruction device	(Consult NSA Evaluated

The listing of NSA Evaluated Destruction Devices for the *terminal* destruction of non-paper COMSEC material can be obtained at: http://www.nsa.gov/ia/mitigation guidance/media destruction guidance/index.shtml or http://www.iad.nsa.smil.mil/library/index.cfm (click on NSA evaluated destruction devices). If necessary, contact the local ~~CMS Advice and Assistance~~ COR Audit Team for assistance. **AMD-9**

12. **Reportable COMSEC Incidents Unique to the CMWS/DMD PS**: The incidents noted below are unique to the CMWS/DMD PS. Operators of the CMWS/DMD PS must promptly report the occurrences below to the IAO/M or EKMS Manager, as applicable

for further reporting in accordance with article 945. If necessary, consult NCMS N5 as to the applicability of incidents reflected in article 945 relevant to the CMWS/DMD PS. Commands are reminded that classified/sensitive IT assets and their proper management and operation are subject to both local command and DON IT directives.

a. **Reportable COMSEC Incidents:**

(1) The introduction of or storage of unencrypted (red) keymat in the CMWS/DMD PS, whether intentional or accidental.

(2) The connection of the CMWS/DMD PS to an unauthorized external or internal communications device (modem or network card) or any device not specifically authorized herein.

(3) Unauthorized access (including failure to properly log off the DMD PS when not in use.

(4) The physical loss of the Secret-high Tier 3 CMWS/DMD PS, its associated hard drive or removable media.

NOTE: Access exists when such a person has the capability and opportunity to gain detailed knowledge of or to alter information or material. A person does not have access if he or she is under escort or if physical controls prevent the person from acquiring such knowledge or modifying information/material.

(5) The sharing of passwords or the use of group accounts are **not permitted** on the CMWS.

(6) Whenever emergency destruction of COMSEC or COMSEC-related material (e.g., CMWS hard drive) is carried out, regardless of the circumstances, and whether or not material may have been compromised.

(7) Use of the CMWS for other than its intended purpose (e.g., CMWS/DMD PS hosting software applications not expressly approved (in writing) for installation and use by the Navy Operational DAA and SPAWAR Program Officer (PMW 160.2).

13. **Taking Operational CMWS Hard Drive Out of Use/Service**: Commands must contact NCMS N3 for disposition instructions for the CMWS hard drive and any remaining accounting requirements

related to the encrypted keys stored on it ***before*** being taken out of use and sanitized using approved methods.

14. **Shipping/Transportation**:

When the CMWS/DMD PS hard drive must be transported or shipped for operational use at another physical location, its movement must be pre-approved by the supporting EKMS Manager/parent account and it must be shipped following the procedures in Chapter 5 for Secret material.

15. **DMD PS UAS Training**:

Information related to CMWS/DMD PS training and quota availability may be obtained through the Center for Information Dominance (CID).

16. **Technical Support**:

SSC-Atlantic will only provide technical support to CMWS's systems that are fielded and issued by SPAWAR. All CMWS platforms issued by SSC-Atlantic will be tracked, registered, and monitored by the serial number(s) of the platform and hard drive. Therefore, in order to obtain user customer support from the SSC-Atlantic Technical Support Helpdesk, users must provide both the CMWS serial number and hard drive serial number.

17. **CMWS Disposition**:

Commands with an EKMS Phase 5 LMD/KP in receipt of a CMWS/DMD PS with no operational requirement to use it to manage Black Key at the account or LE level may contact SSC Atlantic and coordinate return of the unit. Such decision is a command one in which the ISIC should be consulted prior to doing so for any future requirements where the device may be required especially within the aviation community. The originator is responsible for preparation and enclosure of a DD-1149 and OPNAV 5511/10 as well as the shipping cost.

ANNEX AI

OMNI TERMINAL

1. **Purpose and applicability**: To promulgate guidance related to the; acquisition, accountability, safeguarding, handling, storage of OMNI devices.

2. **Description/Use**:

a. OMNI devices are NSA approved Type 1 Controlled Cryptographic Items (CCI) and are continuously accountable to the Central Office of Record (COR) as ALC-1. There are (4)different variants of OMNI each with a different Short Title as illustrated below:

Short Title	Device	Key Order Forms
FNAC21	OMNI	CF Form 1027 (for US) CF Form 1028 (FI)
FNAC30	OMNI	CF Form 1029 (CCEB)
FNAC40	OMNI	CF Form 1030 (NATO)
FNAC50	OMNI	CF Form 1031 (COALITION)

b. The OMNI is a Future Narrow Band Digital Terminal (FNBDT) compatible device designed to provide secure voice and data connectivity with wired or wireless FNBDT compatible equipment supported by a host telephone line.

c. When properly keyed, the OMNI terminal is approved to protect information of all classifications and categories.

3. **Security Features**: The OMNI terminal offers many of the same features found in other secure voice products (i.e. STE, SECTERA, etc…) including but not limited to;

a. **Secure Access Control System (SACS)**: SACS features are designed to allow for controlling secure connections based on capabilities and privileges of the terminal. This feature may be invoked following the vendors procedures in the user manual for either attended or unattended operation. Unattended operations requires that the SACS feature be enabled.

b. **Access Control List (ACL)**: When SACS is enabled, this feature enables the device to be pre-configured with a list of remote terminals which is authorized to establish secure sessions with the terminal.

c. **Minimum Security Level (MINSL)**: When SACS is enabled, this feature prohibits a secure session from a terminal with a key classified lower than that set in the MINSL configuration of the terminal in which the connection is attempted.

d. **Maximum Security Level (MAXSL)**: When SACS is enabled, this feature prohibits a calling terminal from using a key classified higher in classification than that loaded in the receiving terminal or reflected in the MAXSL security setting.

4. **PIN Information and Management**: OMNI devices are received with the COMSEC software disabled by default. The Terminal Administrator (TA) if appointed, LE Issuing or EKMS Manager must use the default TA PIN “3141592” to create a unique seven digit TA pin.

a. Following creation of a TA PIN, the TA, LE Issuing or EKMS Manager, as applicable can load keying material into the device, create an Authorized User (AU) account, program AU privileges and configure applicable security features.

b. Both TA PINS or AU PINS can be changed at any time by an authorized TA (or EKMS Manager) or AU. The AU PIN must consist of six digits.

c. The TA PIN is required for loading, configuring and programming the device. It cannot be used to unlock either the secure voice or data modes. These features or operational use of the device requires a valid AU PIN.

d. AU PINS must follow appropriate DoD Passwords guidelines set forth in the DoD Password Management Guide (CSC-STD-002-85).

e. PINS must be changed at a minimum of every 90 days or more frequently when required by local policy or when necessitated by; transfer, separation or retirement of someone with the current PIN, or when compromised or suspected to have been subject to compromise.

f. PINS will not be written down, affixed to or written and left in the vicinity of the device where an unauthorized person may gain access. If written down, such will be done on a SF-700 and safeguarded, stored and inspected in accordance with Article 515.f.

g. The EKMS Manager, LE Issuing or Security Manager, as applicable is authorized to create and maintain a list of; TA PINS, AU PINS, Key Management Identification Numbers (KMIDs), and OMNI Terminal serial numbers. This list must be marked, safeguarded and stored based on the highest classification of key loaded in the equipment reflected on the list/sheet.

h. If a User enters the AU PIN incorrectly four consecutive times, the device must be returned to either the TA, LE Issuing, or EKMS Manager as applicable who can create a new AU account and PIN to negate having to reload the device.

i. If the TA PIN is entered incorrectly four consecutive times, the terminal will be locked out and the keying material will be zeroized. The device will have to be re-initialized and reloaded, as well.

5. **Classification**:

a. An OMNI terminal is classified based on the highest classification of key filled in the device when a user is logged on (through entry of a valid PIN).

b. When not logged or/the secure functionality of the device is disabled, the device is unclassified CCI.

c. Whether logged on or when the secure functionality is disabled, the device must be safeguarded, stored and handled in accordance with Chapter 5.

6. **Security Awareness**: Users of OMNI terminals must remain cognizant of their surroundings, as well as personnel in the vicinity when classified information is discussed to prevent such information from being overhead by others who may not have the appropriate security clearance and/or need to know.

Additionally, users must verify the device is in the secure mode at the appropriate level prior to passing classified information and also not exceed the classification level indicated in the terminal LED.

In a high risk environment, additional security procedures including but not limited to; the use of NSA applied tamper seals and consultation with the Information Assurance Manager (IAM) regarding approved devices and documentation requirements for connecting a OMNI Terminal to standalone or networked computer to prevent violating any inter-connection requirements or the Systems Security Authorization Agreement (SSAA).

7. **Validation of requirements**: Will be in accordance with Article 610.

8. **Access**:

a. Access to COMSEC material, including OMNI devices is restricted to properly cleared, authorized and trained personnel in accordance with Article 505.

b. LE Personnel will comply with the provisions reflected in Article 465.

c. COMSEC material will not be issued to contractors from a DON EKMS account without ensuring all provisions set forth in OPNAVINST 2221.5(series) and Articles 505.f and 505.g, as applicable are complied with.

d. COMSEC material will not be released to foreign nationals without appropriate approval from NSA/DP02 as discussed in Article 505.

e. As the ONMI device does not permit extraction of key, Two Person Integrity (TPI) is not required for access to the device or use of the device in the secure mode. However, TPI is required when the device is loaded with T.S. keying material as discussed Article 510.

9. **Keying Management (Ordering, Forms, Distribution, Loading, and Management)**: Unlike traditional keying material which is auto distributed based on an accounts validated allowance and distribution profile, keying material for use in OMNI devices is considered modern key and **MUST** be ordered to ensure required keying material is distributed to the account.

a. **Ordering:** Will be typically performed by the EKMS Manager or Alternate but in either case the individual ordering modern key must be privileged to place such orders as reflected in the accounts User Registration data on file at the EKMS Central Facility (CF). Keying material may be ordered either by; faxing the request to the EKMS CF, via the LMD/KP or through the interactive online-ordering function located at the URL in 8.b below.

NOTE: For additional information regarding the establishment of privileges for ordering modern key, see Annex AE.

b. **Forms**: Forms used to order keying material for OMNI terminals is reflected in paragraph 2.a above. These forms and applicable guidance on establishing key order privileges can be found at: https://www.iad.gov/Keysupport/index.cfm

c. **Distribution**: Modern keying material is delivered to requesting and authorized accounts via the X.400 message server associated with the LMD/KP.

d. **Key Loading**: Will be performed by the EKMS Manager, Alternate or LE Issuing, as applicable via a DTD, SDS, or SKL using a NSA authorized and TEMPEST-approved key loading cable.

NOTE: TPI handling and storage requirements set forth in Article 510 must be adhered to when loading Top Secret keying material from a DTD, SDS, or SKL.

e. **Key Management**: It is highly recommended that the EKMS Manager maintain either a spreadsheet or database to record the key loaded in a OMNI reflecting the KMID and serial number of the device in which the key was loaded. Alternatively, the data can be reflected in the remarks or comments field on the SF-153 used to issue the OMNI from LCMS at the time of issue. If the device is lost, stolen or otherwise compromised, the EKMS Manager will provide the KMID and OMNI serial number to the EKMS CF to have the KMID added to the Compromised Key List (CKL) database at NSA.

f. **Key Rekey**: A rekey is required at a minimum of annually, prior to expiration of the key loaded or when directed by the EKMS CF. Failure to do so or if the device is zeroized or another key of a different classification is required, the device must be reloaded with a new key from the DTD, SDS, or SKL, as applicable.

NOTE: The following numbers are available for performing rekeys of OMNI terminals: (Toll Free) 1-800-633-3971, (Comm) 410-526-3470, (DSN) 312-238-4470. Numbers are subject to change however, up-to-date numbers and guidance for loading and performing rekeys can be found at: https://www.iad.gov/Keysupport/index.cfm

10. **Issuance and Accountability**:

a. All issuance and returns will be handled by the EKMS Manager/Alternate or LE Issuing, as applicable and accomplished following proper local custody procedures set forth in Article 769.

b. The EKMS Manager must ensure that personnel are appropriately cleared and authorized such access in accordance with Article 505.

c. Local custody documents for both issues and returns will be retained in accordance with Annex T.

d. Like other CCI equipment, OMNI devices will be inventoried at a minimum in accordance with Articles 766, 775 and 778, as applicable.

11. **Shipping**:

a. OMNI Terminals will be shipped in accordance with Article 535.

NOTE: Unlike legacy COMSEC equipment or equipment which permits key extraction, **OMNI Terminals may be shipped in either a keyed or unkeyed state however, when keyed the secure mode must be disabled.**

b. Under **no circumstances** will PINS be shipped with the associated equipment.

c. Cleared and authorized courier personnel may be used to transport OMNI terminals in accordance with Article 530.

12. **Procedures for Failed Devices**: Users experiencing problems will request assistance from the Terminal Administrator (TA), LE Issuing or EKMS Manager, as applicable.

a. Local maintenance of OMNI devices is **NOT** authorized.

b. If the device is found to be defective and unable to be restored to service by the TA, LE Issuing or EKMS Manager, as applicable, it will be returned following proper local custody procedures set forth in Articles 712 and 769 of this manual.

c. EKMS Managers must follow applicable procedures in EKMS-5 Chapter 4 in requesting disposition instructions for failed units.

d. Under no circumstances will any OMNI Terminal be opened or attempted to be opened. If discovered, such must be reported in accordance with Article 945.E and this Annex.

e. Prior to shipping a OMNI for repair or replacement, the TA, LE Issuing or EKMS Manager must verify that all keys and user data has been deleted and power down the device.

NOTE: If the keying material cannot be deleted or the device cannot be zeroized, the device will be shipped based on the highest classification of key possibly still in the device at a minimum Secret level.

13. **Emergency Actions**: In the event of impending site overrun and/or capture, zeroize the OMNI Terminal. Then, as time permits, destroy the device beyond use (smash with a fire axe, hammer, or other heavy object).

14. **Reportable COMSEC Incidents**: The loss, theft, unauthorized access, evidence of tampering or unauthorized maintenance or attempted maintenance of an OMNI Terminal must be reported in accordance with Article 945.e.

ANNEX AJ

INVENTORY RECONCILIATION (PROCESSES AND PROCEDURES)

1. **Purpose and applicability**: To provide guidance for EKMS Managers in the processes and procedures used to reconcile discrepancies listed on the EKMS account's Inventory Reconciliation Status Transaction (IRST). Failure to self-reconcile within 90 days must be reported in accordance with Article ~~945.e.16~~ 1005.a unless an extension has been granted by NCMS, in writing.

AMD-9

2. **IRST Description**:

a. The IRST is an automatically generated report created by the Common Tier One (TIER-1) system upon receipt of an EKMS account's (TIER-2) inventory report.

b. The IRST will list all discrepancies or inconsistencies between the inventory report submitted by the EKMS account and that of the TIER-1/COR account data for the respective account.

c. The IRST will reflect; what material is listed as either EXCESS or SHORT for the EKMS account and also what material is listed in-transit (IT) to the EKMS account.

NOTES: (1) Terms appearing within this annex as hyperlinks are further explained in EKMS-1(Series) glossary.

(2) Throughout this annex where reference is made to submission of accounting reports to the COR/Tier-1, such reference implies via the X.400 message server.

3. **IRST Reconciliation Processes**:

a. **Reconciliation Step-by-Step Procedures**

1. Upon receipt of a Request Inventory Transaction (RIT) from Tier-1 for either a SAIR or CCIR; Select Accounting → Inventory → Process Electronic Request Inventory. Then select the request inventory transaction and click "Select Transaction". In the 'Process Electronic Request Inventory' window, enter any desired comments, then click "Prepare Inventory Report". Once icon appears, wrap the resulting icon on the desktop and send it to your Central Office of Record

(COR) either 616502 or 5A8240. (**DO NOT SELECT YOUR OWN SIX DIGIT ACCOUNT**).

2. After wrapping and sending the inventory, an IRST is automatically created requiring the account to download, unwrap, and print (both types of IRSTs (free format text version and a SF-153 version are created)).

3. The Account Manager must close the open inventory by processing the IRST in the LMD. To process a received Inventory Reconciliation Status Report, perform the following steps from the LCMS desktop.

Select **Accounting->Inventory->Process Electronic Reconciliation Status**.

4. Next, review the bottom of the free format text version of the IRST where the transactions are listed and compare them to the Inventory report. To do so, open the electronic inventory transaction used to create that particular IRST from the LCMS desktop. On the inventory report top right side of the inventory look for a field marked reportable transactions with account number, date and transaction numbers. There are also three dots (...) at the end of the field. Click on this button and a drop down menu will appear. This is a list of all of the transactions that were used by LCMS to create that inventory. Copy all of the transactions on a separate piece of paper. Match these transactions to the ones located on the bottom of the free format text IRST. If they do not match, restore the icons for those transactions not listed on the IRST from the Transaction Status Log. Next, wrap and send these transactions to the COR/TIER-1.

5. Once all transactions have been sent using the above procedures, submit a Change of Account Location (COAL) Inventory to the COR using the procedures outlined in EKMS 704 (series). If the transactions sent are still listed on the IRST, contact a COR manager or the NCMS Accounting Division (TEL: 240-857-7230/9055; EMAIL: ncms_nafw_cor@navy.mil. A COR representative will advise the Manager as to what, if any transactions must be sent or resent to the COR/TIER-1.

4. **PROPER AND TIMELY RECEIPT OF MATERIAL IS ONE OF THE MOST IMPORTANT STEPS IN THE IRST RECONCILIATION PROCESS.** On a monthly basis, a Pending Receipts Report is sent to each account automatically via x.400. If material has been received but remains reflected on the Pending Receipts report, the corresponding receipts for the material must be submitted to TIER-1/COR. If the material has not been received, and it is an electronic Short Title, it may be an indication of a BAD BET.

> **NOTE: Timely and proper receipt of material which is "IT" is important and directly impacts other transactions such as destruction or transfer reports. Material cannot be properly destroyed or transferred until it has been properly receipted for.**

a. **Processing Short Items.** After completing the above step-by-step procedures, COMSEC material may still be listed on the IRST which needs to be reconciled. The below procedures provide both insight and guidance in resolving items listed as short on the IRST. Short items on the IRST will normally be listed in the following manner:

1. **T1: 1-On-Hand, T2: None**

POSSIBLE CAUSE: Destruction or transfer reports were not submitted to the COR/TIER-1.

SOLUTION: Verify that the material was either destroyed or transferred, if so; resubmit the applicable accounting reports to the COR/TIER-1.

2. **T1: 4-On Hand, T2: 2-On Hand (ALC-2 items)**

POSSIBLE CAUSE: Inaccurate quantity for the material reflected on the inventory report; destruction or transfer reports for some of the material were not submitted to the COR/TIER-1.

SOLUTION: Verify the actual quantity of material on-hand. Once verified (visually) submit the applicable accounting reports related to the quantity discrepancy noted on the inventory report i.e. destruction report, transfer report, etc. to the COR/TIER-1.

IRST LEGEND:

A. T1 IS TIER-1; T2 IS TIER-2 i.e. UNIT EKMS ACCOUNT;
B. LETTERS K OR E PROCEEDING 'ON-HAND' ARE K = KEY AND

E = EQUIPMENT;

C. NUMBER PROCEEDING 'ON-HAND' (1-ON-HAND) IS QUANTITY OF MATERIAL BEING ADDRESSED (ALC-2 ONLY).

3. **T1: 1-IT, T2: None**

POSSIBLE CAUSE: Material has been sent to the EKMS account by another account who submitted the transfer report individual (TRI), but, the receiving account has yet to receipt for the material by submitting either a transfer report receipt all (TRRA), transfer report receipt individual (TRRI), or transfer report receipt exception (TRRE); or the receiving EKMS account has not received the material.

SOLUTION: If the material was received, process a TRI by submitting either a TRRA or TRRI, as applicable for material to the COR/TIER-1.

NOTE: There are additional situations that can result in an item to be listed as short on the IRST including but not limited to either an incorrect short title or ALC entry on the EKMS account's inventory report. When discovered, these discrepancies can be resolved using the procedures outline in this annex under 'Procedures to Perform Reliefs and Possessions'.

4. **T1: K-On-Hand; K-IT; T2: K-On-Hand (IT - 880XXX DATE TN)**

POSSIBLE CAUSE: Material (usually ALC 6) sent to account on two separate transactions [TRIs] but only receipted on one. (System failure, system restore, or Bad Bet).

SOLUTION: Determine if a Bad Bet was reported, or that LMD was down during the timeframe of the transaction in Parenthesis on IRST (i.e. **IT - 880XXX DATE TN)** and provide that information to your COR.

5. **T1: K-DZ; T2: None; (DZ – 169XXX DATE TN)**

Short titles associated with the above code will likely also be reflected in the IRST with the below code as well.

T1: K-IT; T2: None (IT – 880XXX Date TN)

POSSIBLE CAUSE: Material (usually ALC 6) sent to account on two separate transactions [TRIs] but only receipted on one. (System failure, system restore, or Bad Bet). Account has since destroyed short title and reported destruction to the COR. *SOLUTION:* Determine if a Bad Bet was reported, or that LMD was down during the timeframe of the transaction in Parenthesis on IRST (i.e. **IT - 880XXX DATE TN)** and provide that information to your COR.

b. **Processing Excess Items**

1. Upon completion of the above procedures, COMSEC material may still be listed on the IRST that must be reconciled. Excess items on the IRST are normally reflected as illustrated below and can be resolved through the procedures which follow the descriptions below.

2. **T1: NONE, T2: E On-Hand**

POSSIBLE CAUSE: Material has not been properly accounted for, such as account failed to submit either a TRRA, TRRI or possession report, as applicable to the COR/TIER-1.

SOLUTION: Restore the transaction either TRRA, TRRI, or possession report, as applicable from the Transaction Status Log to desktop and wrap/send it to the COR/TIER-1.

3. **T1: 7-On Hand, T2: 9-On Hand(ALC-2 items)**

POSSIBLE CAUSE: The quantity of the material held is inconsistent with that reflected in the inventory report; TRRA or TRRI not submitted to COR/TIER-1; or the material was brought into accountability with a possession report, however, but the possession report was not sent to the COR/TIER-1.

SOLUTION: Verify the quantity of material on-hand. Once verified (visually) submit the applicable accounting report(s) related to the inventory report, i.e. TRRA, TRRI, or possession report to the COR/TIER-1.

4. **T1: K-IT, T2: K On-Hand**

POSSIBLE CAUSE: Material has been sent to the EKMS account by another account who submitted the transfer receipt individual (TRI)and although the receiving EKMS account did receive the material, a receipt was not sent to the COR/TIER-1.

SOLUTION: If in receipt of the material, the receiving EKMS account must submit a TRRA or TRRI to the COR/TIER-1.

5. **Relief from Accountability (RFA) and Possession Reports**:

Occasionally, it may be discovered that errors or anomalies exist which span back in time beyond the retention requirements set forth in Annex T of this manual necessitating the need to utilize either a Relief from Accountability or Possession Report to have the item removed or brought on charge to the account.

See Articles 739 and 745 regarding the use of either Possession Reports or Relief from Accountability reports, including purposes and required authorization for both.

Reconciliation Glossary:

Destroyed-Zeroized (DZ): A term which pertains to material ALC 1 or ALC 6 that has been sent to Tier 2 Account on more than one transaction [TRIs], one of which was correctly receipted and later material destroyed and reported destruction to COR. The other transaction is still OPEN pending a receipt or cancel distribution at COR.

Excess: Excess items pertains to those items reflected on the IRST which are held by the account, however, the account did not submit the applicable accounting report to the COR/Tier-1 to have the item properly charged.

In-transit (IT): A term which pertains to material in which a TRI was created and sent to the COR/Tier 1 but has yet to be receipted for by the receiving account to the COR/Tier-1.

Inventory Reconciliation Status Transaction (IRST): Is an automatically generated inventory discrepancy listing. The IRST will reflect material which is either short or in excess. The IRST is generated when the EKMS Manager submits the Inventory Report transaction; the TIER-1 system then receives the transaction and compares the inventory with the account's TIER-1 summary account.

Pending Receipts Report: A report which is automatically-generated either monthly or manually by a Tier-1 COR manager. The report is used to provide EKMS accounts a listing of TRI's shipments to their account and also reflects COMSEC material that has not been receipted for to the COR/Tier-1 by the EKMS account.

Short: Pertains to material which is still being tracked by the COR/TIER-1 system but is no longer accounted for by the EKMS account /TIER-2.

Transfer report individual (TRI): A transaction report used to document the transfer of material from one EKMS account to another. EKMS accounts transferring material **must** ensure a copy of TRI is sent to the COR/TIER-1.

Transfer report receipt all (TRRA): Is used to receipt for ALL material reflected on an electronically-generated TRI. Material is receipted for by the receiving EKMS account upon actual receipt of the material. Submission of a TRA certifies the TRI and material received match, and there are no exceptions.

Transfer report receipt exception (TRRE): Is used to process a receipt indicating partial receipt of the material listed on the electronically-generated TRI. The receiving EKMS account will select the material that has not actually been received; all others will be added to the receiving accounts inventory. For additional information on TRREs, see Articles 727, 742.A.2 and 754, as applicable.

Transfer report receipt individual (TRRI): Is used to receipt for individual items listed on a manually-generated TRI. The material is receipted for by the receiving EKMS account upon actual receipt of material as listed on the TRI.

INDEX