DEPARTMENT OF THE NAVY
COMMANDER MILITARY SEALIFT COMMAND
914 CHARLES MORRIS CT SE
WASHINGTON NAVY YARD DC 20398-5540

REFER TO:

COMSCINST 2000.2 CH-1
N6
6 March 2003

COMSC INSTRUCTION 2000.2 CHANGE TRANSMITTAL 1

Subj: COMMUNICATIONS POLICY AND PROCEDURES MANUAL (CPPM)

Encl: (1) New pages vii thru xviii, new Chapter 8

1. Purpose. This change incorporates a new chapter into the basic instruction. This chapter provides MSC-wide policy and procedural direction for operation of its Electronic Key Management System (EKMS) in support of DoD and DoN Communications Security (COMSEC). This chapter provides MSC guidance to afloat and shore-based commanders, commanding officers, ships' Masters and other MSC activities whom are required to handle COMSEC related material or perform functions.

2. Action. Remove pages vii thru xvi of the basic instruction and insert enclosure (1) as appropriate. Insert new Chapter 8 after page 7-21 of the basic instruction.

//S//
D. L. BREWER III

Distribution:
COMSCINST 5215.5
List I (Case A, B, C)
SNDL 21A (Fleet Commanders in Chief (N6))
41B (MSC Area Commanders)
41C (NFAF East/West)
41D (MSC Offices)
41E (APMC)
41J (OICMILDEPTs)
41K (APSRON FOUR)
41L (COMPSRONs)
41M (TAGOS Project Office)
T-100 (Masters, civil service manned ships)
T-102 (Masters and Operators, contract-operated Fast Sealift Ships)
T-103 (Masters and Operators, contract-operated TAGOS)
T-104 (Masters and Operators, contract-operated MPS)
T-105 (Masters and Operators, contract-operated LMSRs)
T-106 (Masters and Operators, contract-operated Prepo)
T-107 (Masters, civil service manned Fast Combat Support Ships)
USTRANSCOM (J6)
MARAD
All time chartered ships

CHAPTER 8 - MSC INFORMATION SECURITY (INFOSEC) AND COMMUNICATIONS SECURITY (COMSEC) MATERIAL SYSTEM (CMS) POLICY AND PROCEDURES

Communications Policy and Procedures Manual

Table of Contents

List of Effective Pages

Page Number	Change Number
Title Page	Original
Letter of Promulgation	Original
i thru vi	Original
vii thru xviii	CH-1
1-1 thru 1-2	Original
2-1 thru 2-16	Original
3-1 thru 3-13	Original
4-1 thru 4-20	Original
5-1 thru 5-17	Original
6-1 thru 6-34	Original
7-1 thru 7-21	Original
8-1 thru 8-55	CH-1
A-1 thru A-8	Original
B-1 thru B-11	Original
C-1 thru C-8	Original
D-1 thru D-10	Original
E-1 thru E-9	Original
F-1 thru F-5	Original
G-1 thru G-17	Original
H-1 thru H-13	Original
I-1 thru I-71	Original
J-1 thru J-6	Original
K-1 thru K-12	Original

CHAPTER EIGHT

MSC INFORMATION SECURITY AND COMMUNICATIONS SECURITY MATERIAL SYSTEM POLICY AND PROCEDURES

8.1 Purpose and Scope

The purpose of this chapter is to provide MSC-wide policy guidance and the procedural information necessary for communication system users to effectively manage the handling of communications security (COMSEC) cryptographic keying-material. This chapter provides MSC guidance to afloat and shore commanders, commanding officers, ships' Masters and others who are required to handle COMSEC material. The administrative and operational procedures required to meet the needs of information assurance and security standards, as well as, for the proper operation of the U.S. Government's Electronic Key Management System (EKMS) including sample forms are also provided in this chapter.

Information security (INFOSEC) is increasingly at risk in view of the accelerating barrage of technological changes in communications and information processing. The information security concerns of the U.S. government must deal with increased complexity, constant change, information overload, and limited expertise in security matters. Starting with the Office of Management and Budget (OMB) Circular A-130, then the National Security Agency's Information Assurance Technical Framework programs, next the DODD 5200.28 of 21 Mar 88 on Security Requirements for Automated Information Systems and finally the U.S. Navy security regulations; a comprehensive collection of rules and regulations has been condensed in the following to the items of specific concern to MSC operating units.

The scope of this chapter covers MSC policy and procedures concerning:

- COMSEC Material System (CMS) Management Structure
- EKMS Implementation
- COMSEC Material Handling, Accounting and Physical Security
- Access and Security Clearance Requirements
- Training
- Audits and Assist Visits
- Emergency Action Planning
- Secure Telephone Unit and Secure Terminal Equipment
- Data Transfer Devices

8.1.1 Background

As described in Chapter Three, MSC has some unique INFOSEC and COMSEC implementation requirements resulting from the diverse manning circumstances found on government-owned/government-manned, government-owned/contractor-operated, U.S.-owned chartered and foreign-owned chartered ships. Personnel having proper security clearances, who also require access to communications cryptographic material, must also have specialized COMSEC authorization, appointment and training.

Historically, MSC has maintained independent CMS custodial accounts at each of the individual ships and at the staff levels. After a study of the requirements and the testing of a revised CMS management-concept, MSC instituted a program to streamline CMS operations. This program supports MSC initiatives to reduce the workload and some of the training requirements. In 1999, MSC consolidated the shore-side CMS accounts after having established a centrally managed EKMS Tier 2 account under the new DoD system. This centralized EKMS Tier 2 account management-structure is being expanded in its operation to provide services to MSC ships, staffs and deployable units worldwide. Some of the benefits of creating a single central account include:

- Reduction of the need to carry keying material items previously required to be held in anticipation of future operations as a Reserve-On-Board (ROB);
- Use of electronic over-the-air-transfer/over-the-air-receipt (OTAT/OTAR) of COMSEC keying material, vice physical transfer, thereby improving timeliness;
- Streamlining procedures for transfer, operational-handling, storage and accountability for COMSEC material;
- Elimination of small CMS accounts that require more-specialized training (EKMS Managers school) and
- Provision of more expertise and improved timeliness of response to unit's CMS support requirements with a greater role being played by a MSC representative in the Area of Responsibility (AOR) where the unit is operating.

8.2 DoD INFOSEC and CMS Management Organizational Structure

8.2.1 INFOSEC

SECNAVINST 5510.36, DON Information Security Program Regulation, establishes the DON Information Security Program (ISP). The ISP applies uniform, consistent and cost-effective policies and procedures for the preparation, classification, safeguarding, transmission and eventual destruction of classified information. It also provides guidance on security awareness education and the national industrial security program. The term "classified information" includes classified "material" (i.e., any matter, document, product or substance on or in which classified information is recorded or embodied). The underlying security maintenance principle is strict compliance to the rule that access to classified information is restricted to only certain individuals based on first, appropriate clearance and second, a need to know.

As equipment technology for the EKMS matures, the automation of information security assurance administrative procedures become an integral part of both the overall DON ISP and MSC ISP.

COMSCINST 5510.8F, COMSC Information and Personnel Security Regulation; COMSCINST 5522.1, Random Security Inspection Authorization; COMSCINST 5530.3B, MSC Ship Physical Security; and COMSCINST 5530.4, Physical Security Plan provide additional details on INFOSEC-related matters.

8.2.2 Communications Security (COMSEC) Material System (CMS)

COMSEC is defined as actions taken to deny unauthorized persons information derived from telecommunications of the U.S. Government concerning national security, and the measures to ensure the authenticity of such telecommunications. (NOTE: COMSEC also includes cryptographic-security, emission security, transmission security and physical security of COMSEC material as well as COMSEC information itself.)

COMSEC material is that material used to protect U.S. Government transmissions, communications used in the processing of classified or sensitive unclassified information, related to national security, from (access by) unauthorized persons and that material used to ensure the authenticity of such communications.

The protection of vital and sensitive information moving over/through 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 cryptographic-production facilities, the COMSEC Central Office of Record (COR), distribution facilities (i.e., depots) and CMS operational-level accounts, is known collectively as the COMSEC Material Control System (CMCS).

Material is managed in numerous COMSEC accounts throughout the Federal Government, as well as, the civilian sector supporting the Federal Government.

8.2.3 Electronic Key Management System (EKMS)

The existing CMS is being replaced by the new EKMS. During the current transition, the top level of the EKMS/CMS administrative/operational management-structure is as follows:

- The National Security Agency (NSA) is the executive agent for developing and implementing national level policy affecting the control of COMSEC material. The NSA is also responsible for the actual production and initial distribution of most COMSEC material.
- DON administers its own CMCS which includes the Navy, the Marine Corps, the Military Sealift Command and the Coast Guard CMS Accounts. The DON CMCS implements Navy policy, publishes procedures, establishes its own COMSEC accounts (referred to as CMS accounts) and provides a COR to account for all COMSEC material.
- The Chief of Naval Operations (CNO) has overall responsibility and authority for implementation of the national COMSEC policy within the DON. On the Navy staff, the Head, Navy Information Security Branch (N643) acts as the sponsor for COMSEC resources and is responsible for consolidating the COMSEC financial requirements programming, planning, as well as, the implementation of policy and coordination of technical improvements.

- The Director, Communications Security Material System (DCMS) administers the DON CMS program and acts as the Navy's COR for all the DON CMS accounts. The DCMS's staff performs a wide range of functions to implement, support and monitor the performance of the system.
- The EKMS Central Facility (CF) functions primarily as a high-volume cryptographic key distribution and sometimes generation center. As such, it provides the commands with keys, which are produced by NSA, or that cannot be generated locally. The CF will inter-operate with local commands utilizing a variety of media, communication devices and networks, which ultimately will allow for the automated ordering of COMSEC keys and other materials, which are generated and distributed by the NSA.
- The Controlling Authority (CA), in the context of the CMCS, ensures that each individual item of COMSEC material is controlled or managed. By definition, a CA has the command-delegated responsibility for directing the establishment and operation of a crypto-covered net/circuit and managing the operational use and control of keying material assigned to a crypto-covered net/circuit. A CA is responsible for evaluating COMSEC incidents and authorizing the issue/destruction of COMSEC material under his/her control.
- The Immediate Superior in Command (ISIC) for all activities under his command is the Commander, Military Sealift Command (COMSC). As the ISIC, he is responsible for the administrative oversight of all CMS matters conducted by the subordinate commands. He has assigned this responsibility to a senior staff member in the command's N6 staff organization with oversight by the MSC N6 Director.
- The designated Staff CMS Responsibility Officer (SCMSRO) for MSC is a senior person on the N6 staff appointed on the basis of ability and experience. SCMSRO policy, responsibilities and functions are defined in sections that follow covering Management Functional Roles and Procedures in Section 8.5.1.1.
- The EKMS Manager and the Alternates for MSC are specifically designated N6 staff members whose responsibilities are defined in Sections 8.4.1 and 8.5.1.2.
- The MSC Area Commanders, Squadron Commanders, ships' Masters and officers in charge (OICs) of mobile units, plus the Commanders ashore, are responsible for properly administering their command/activity (local element (LE)) CMS holdings and ensuring compliance with this instruction. This organizational level is the key to performing the critical COMSEC functions of appointing custodians, designating personnel for authorized access and ensuring training, audits and the general EKMS administration is completed.

8.2.4 EKMS Organizational Hierarchy

The EKMS itself 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 keys and other types of COMSEC material. The overall EKMS organizational structure consists of four layers:

- TIER 0 (Central Facility) – This level is a composite of NSA's Fort Meade, MD and Finksburg, MD cryptographic-key production facilities which provide centralized key-management services for all forms of keys. An initiative for NSA to become the sole centralized manger for both National and Joint international key-management services is expected to reduce the current role of the Navy's DCMS.
- TIER 1 - This is the layer of the EKMS that serves as an intermediate key generation and distribution center, central office of records, privilege managers and registration authorities for COMSEC accounts. Management of the Tier 1 system is a cooperative effort involving the Army, Navy, Air Force, NSA and the Joint Staff (J6). Until such time as the Common Tier 1 system becomes fully operational, CORs will perform many of these functions.
- TIER 2 - This layer of EKMS is comprised of the COMSEC accounts administration staff that manages key and other COMSEC material. Tier 2 accounts are equipped with a Local Management Device (LMD) that utilizes Local COMSEC Management Software (LCMS) which interfaces with the Key Processor (KP) equipment. This suite of electronic equipment is referred to as an LMD/KP.
- TIER 3 – This is the lowest layer of the EKMS organizational structure. This layer provides services which involve use of the Data Transfer Device (DTD), as well as, other technical means used to fill keys into end-user cryptographic peripheral units; issues material to "hard-copy-material-holdings-only" units; and supplies "STU III-material-only-using" units/local entities (i.e., LEs). Unlike LMD/KP Tier 2 accounts, Tier 3 using entities never directly receive an electronic key from a Tier 1 or Tier 0.

8.3 MSC Implementation of EKMS

8.3.1 EKMS Evolution

The new EKMS was developed by the NSA in response to the technological impacts of telecommunications and computer processing evolutions and their potential for national security service improvements. The DoD and other government agencies were subsequently required to implement the electronic key distribution and management system. The Navy's implementation is a multiphase approach for making these improvements.

- Phase I, use of equipment and procedures that were already in use throughout the Navy, consisting of personal computers (PCs) loaded with the Automated Navy COMSEC Reporting System (ANCRS) and COMSEC Automated Reporting System (CARS) software. This software is designed to automate local record keeping and to provide CMS custodians with the capability for direct electronic reporting of COMSEC material transactions up to the Navy COR located at the DCMS facility.
- Phase II enhanced these processes and equipment by providing the capability to migrate from paper-based key distribution to transmission of electronic keys. Phase II devices and components consist of the following elements:
  - LMD, PCs operating under a Santa Cruz Operation (SCO) version of the UNIX operating system;
  - LMCS;
  - KPs, the KOK-22A and

- Version 3 (V3) Data Transfer Devices (DTD), the AN/CYZ-10.

For Phase II, an EKMS Tier 2 level account is equipped with all these elements (LMD, LCMS, KP and a Ver. 3 DTD). A Tier 2 account is charged with the management and accounting responsibilities associated with the entire EKMS account. Tier 2 operation requires highly skilled and experienced technicians. Training prerequisites include a formal 2-week EKMS Manager Course of Instruction (COI) for the LMD/KP operators.

Tier 3 level personnel utilize the DTD as the primary key management tool and function as a LE. They report to, and are serviced by, the Tier 2 account. There are no formal Tier 3 training requirements; any training and certification deemed necessary are a responsibility of the Tier 2 EKMS Manager.

The Navy's EKMS Account Holder Implementation Plan initially scheduled all the existing Phase I Navy CMS accounts, including MSC, for full EKMS Phase 2 installation. However, based on its own evaluation and operational testing of EKMS Tier 2 accounts vs. Tier 3 local elements, MSC N6 Director saw an opportunity to simplify the CMS accounting and keying-material distribution process for MSC, both the afloat and the ashore users. All MSC ships and many MSC shore activities are categorized as "small" users in view of the limited amount of CMS material they require. The policy of MSC is to take advantage of this opportunity through the implementation of a central Tier 2 EKMS organization which serves all the other MSC LEs as Tier 3 CMS Holders utilizing the EKMS.

Future EKMS development phases will further the process. When EKMS reaches full operational capability, EKMS Tier 2 accounts will be able to receive, store, locally generate and distribute purely electronic keys.

8.3.2 MSC EKMS Concept of Operations

MSC Command, Control, Communications, and Computer Systems Directorate (C4S) has established a staff component whose mission includes primary support of the MSC CMS. Under the direction of MSC N6, the single centralized MSC Tier 2 account manager provides CMS support to both the afloat and the shore LE CMS material holders by utilizing the EKMS.

All MSC commands, remote staff elements and operational units are considered Tier 3 LEs. The functional setting and EKMS keying material flow for the MSC concept is shown in Figure 8-1. Support to the various Tier 3 units is implemented through creation of "Primary Tier 3 EKMS Managers for the LEs" in specific regional AORs. These "managers" provide support to all the LEs located or operating in their AOR. These supported LEs are organizationally identified as the "Secondary Tier 3 LE Holders." This decentralized means of support facilitates efficient and timely response to users keying-material requirements. It will also improve EKMS planning, holder and user training and contingency operation EKMS support.

The COMSC EKMS Account Manager, located at Camp Pendleton, Virginia Beach, VA, manages the MSC central CMS Tier 2 account and is the single point of contact for the Tier 1 COR. The Tier 2 EKMS Manager provides COMSEC material to the Primary Tier 3 EKMS Managers. The Primary Tier 3 EKMS Managers subsequently deliver COMSEC material to Secondary Tier 3 EKMS LEs operating in their AOR.

There is a wide range of COMSEC material holdings within the MSC organization. Many of these activities are equipped with only the STU III or STE. Most are already supported directly by the MSC centralized Tier 2 agent. The remaining elements have more extensive COMSEC holdings including those supporting MILSATCOM and tactical circuits. These Tier 2 COMSEC accounts that have been or are being converted to Tier 3.

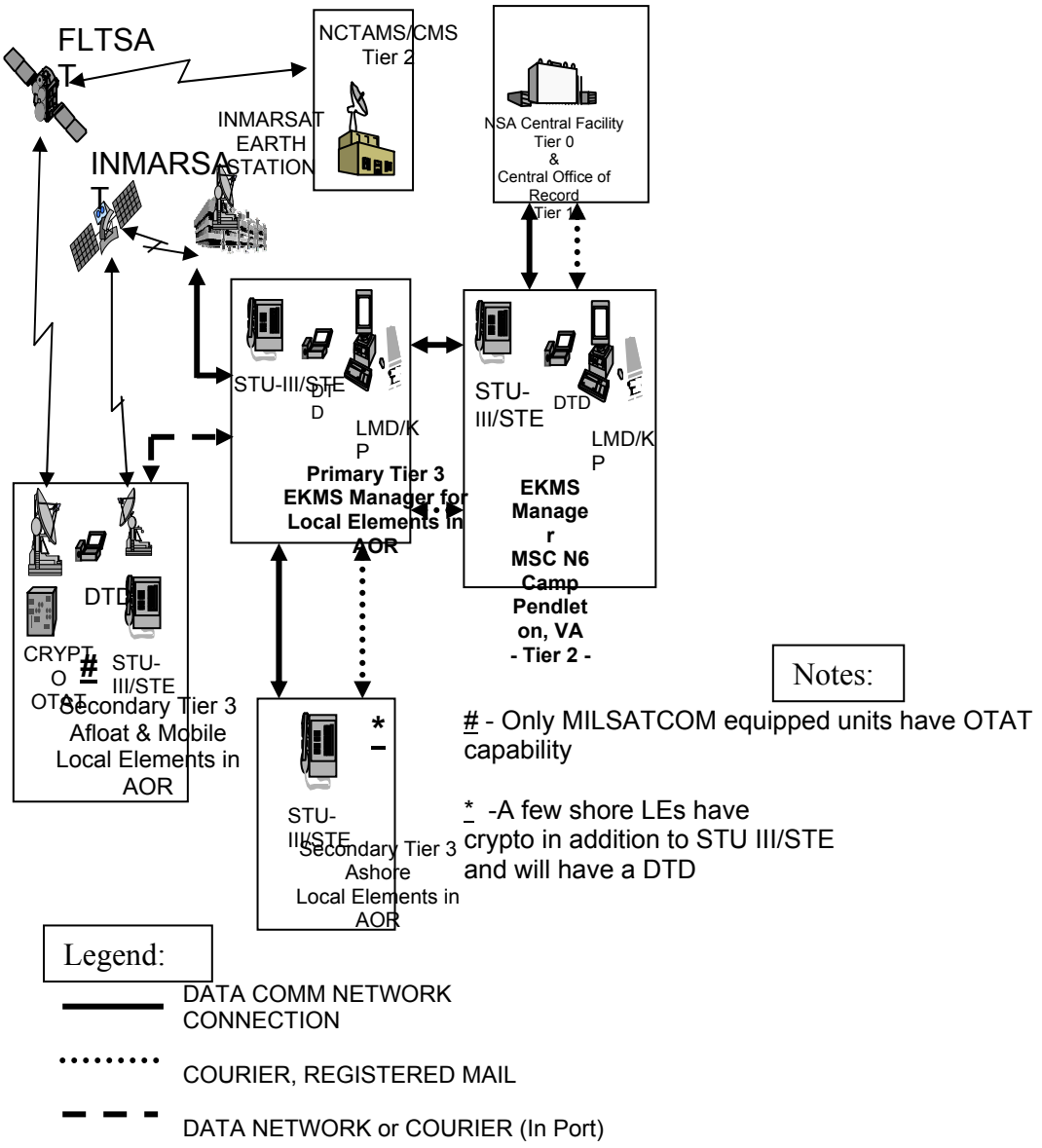

Figure 8-1 MSC Concept of Operations (CONOPS) for Tier 2 Support to Tier 3 LEs

For the Tier 2 MSC EKMS Managers, there are three primary methods for delivery of COMSEC material to the Primary Tier 3 EKMS Managers:

- Physical: Courier, USPS Registered mail or for collocated activities, over the counter;
- Secure Terrestrial network via PTSN and
- Over-the-air-distribution (OTAD) utilizing STU III/STE via INMARSAT.

For the Primary Tier 3 EKMS Managers, methods for COMSEC material delivery to Secondary Tier 3 EKMS LEs are the same, but also include two additional methods:

- For mobile units, over-the-air key material delivery via INMARSAT utilizing STU III/STE is the most widely available method. NCTAMS delivery via the Fleet Broadcast and other selected UHF or other MILSAT Satellite channel related keying material could be via FLTSAT transmission for ships on which this satellite capability is available.
- To provide delivery path redundancy and flexibility, as well as, an alternative means of meeting contingency keying material requirements, material may be forwarded directly to Secondary Tier 3 EKMS LEs by the Tier 2 MSC EKMS Manager.

8.4 MSC EKMS Policy

The paragraph numbering in this section and the numbering in 8.5, MSC EKMS Functions and Procedures, are correlated. The functions and procedures expand on the policy statements and provide required action guidance and references.

8.4.1 Management

The MSC management structure for the EKMS is shown in Figure 8-2.

- MSC N6 will nominate and COMSC will appoint the Staff CMS Responsibility Officer (SCMSRO) to oversee MSC's central CMS/EKMS Tier 2 account # 370006.
- The SCMSRO will appoint in writing the EKMS Manager and Tier 2 Alternates. The MSC EKMS Manager will provide MSC-wide EKMS cryptographic material support for afloat and shore activities. The EKMS Manager is the individual responsible for all actions associated with the receipt, handling, issue, safeguarding, accounting and disposition of COMSEC material assigned to MSC's EKMS centralized numbered account.
- MSC Tier 3 holdings will be managed at two levels, Primary and Secondary.
- Primary Tier 3 EKMS Managers will provide support for ships and mobile units plus MSC shore activities in their AORs. Secondary Tier 3 LEs are all other MSC units.
- Primary Tier 3 EKMS Managers are established in each MSC AOR.
- Area Commanders will appoint, subject to review and concurrence of the MSC SCMSRO, these Tier 3 Primary EKMS Managers in writing.
- Tier 3 Primary AOR EKMS Managers will be responsible for:
  - Consolidating, reviewing and monitoring keying material requirements.

- Distributing keying material.
- Training of personnel to be EKMS LE Holders or users.
- Performing review and assist visits.

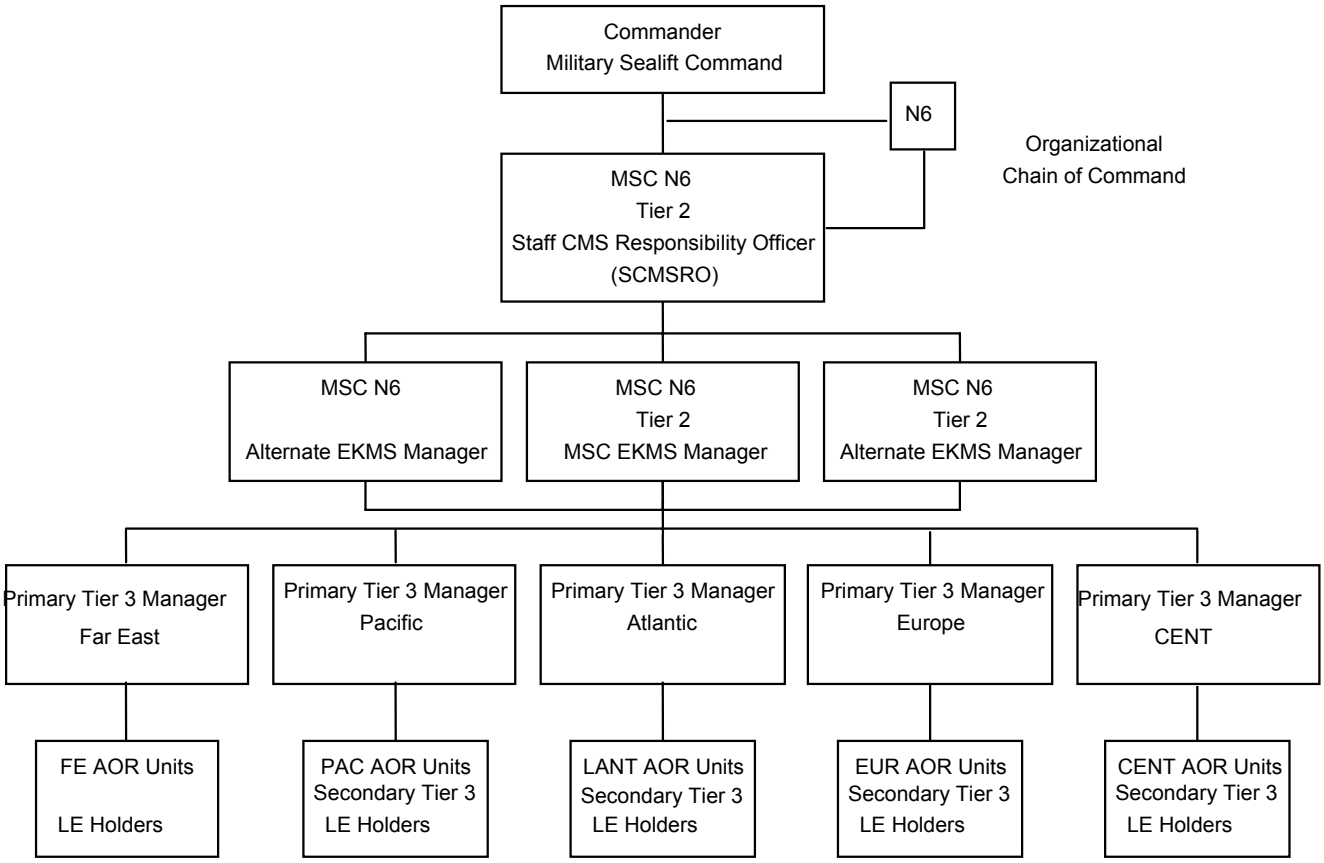

Figure 8-2 MSC Management Structure for CMS and EKMS

- Secondary Tier 3 LE EKMS Holders will be located within Squadron Commander staffs, ships and other mobile units plus designated MSC staff and shore activities.
- The Squadron Commanders, ship's Masters, commanding officers and OICs of mobile units will be responsible for properly administering their command's EKMS holdings and ensuring compliance with established policy and procedures. They will be assisted by:
  - LE Holders who will be the individuals designated in writing by the LE command authority. The holder's chain of management action is via the appropriate Primary Tier 3 EKMS Manager who in turn assists the MSC EKMS Manager and Alternate(s) with routine administrative account matters.

- COMSEC witnesses who will be properly cleared military or civilian personnel who are called upon to assist a LE Holder in performing routine administrative tasks related to the handling of COMSEC/EKMS material. A witness must be authorized access to keying material in writing by the appropriate command authority.
- COMSEC Users who will be properly cleared military or civilian personnel who utilize COMSEC equipment in connection with their official duties. They will be properly trained. They will operate all equipment/systems that utilize COMSEC equipment in accordance with applicable operating manuals and established procedures. They can obtain guidance from the Table 8-3 Points of Contact.

EKMS Area of Responsibility (AOR)	Mail Address	Telephone Number	Message Plain Language Address (PLAD)
World-wide	Military Sealift Command ATTN: EKMS MANAGER C Street Bldg. 243 Camp Pendleton Virginia Beach, VA 23451	757-417-4706 757-417-4700 (Fax)	COMSC EKMS MGR VIRGINIA BEACH VA
Atlantic	Military Sealift Command, Atlantic ATTN: N6 EKMS Manager C Street Bldg.243 Camp Pendleton, Virginia Beach VA 23458	757-417- 4743/4382	COMSCLANT NORFOLK VA //N6//
Pacific	Military Sealift Command, Pacific ATTN: N6 EKMS Manager 140 Sylvester Road San Diego, CA 92106	619-524-9751/9752/ 9997	COMSCPAC SAN DIEGO CA //N6//
Far East	Military Sealift Command, Far East ATTN: N6 EKMS Manager PSC 451 FPO AP 96347-2600	81-311-769-6126	COMSCFE YOKOHAMA. JA//N6//
Central	Commander MSCCENT PSC 451 FPO AE 09834-2800	318-439-4108 (DSN) 318-439-4107 (Fax) 973-724-108 (COMM) 973-724-107 (Fax)	COMSCCENT BAHRAIN //N6//
Europe	Military Sealift Command ATTN: N6 EKMS Manager PSC 817 Box 23 FPO AE 0962-0023	39-081-568-3050	COMSCEUR NAPLES IT //N6//

Table 8-3 MSC Electronic Key Management System (EKMS) Points of Contact

8.4.2 Handling COMSEC Material

8.4.2.1 Use of Over-the-Air Distribution (OTAD) for COMSEC Key Material

It is the policy of MSC to make maximum utilization of OTAD for delivery of COMSEC material to ships and shore-based activities.

Over-the-air-transfer/over-the-air-receipt (OTAT/OTAR) services being offered by the area NCTAMS will be utilized as the primary source of keying material for ships equipped with OTAR receiving capability. Ships using these services will follow the procedures provided by the Area NCTAMS. When a NCTAMS provides the keying material received via OTAT/OTAR from their Tier 2 account, the NCTAMS will account for that material, rather than MSC. No MSC EKMS LE account will further transfer keying material to any other EKMS account without the express written authority of the MSC COMSEC Manager regardless of the source of the material.

8.4.2.2 Custody of Controlled COMSEC Material

It is the policy of MSC to utilize the personnel in the EKMS management hierarchy, defined above, to be holders of Cryptographic Controlled Items (CCI). Distribution as well as maintenance and repair of CCI will be done within the MSC EKMS management structure. Only certified technicians and shore activities designated by the MSC EKMS Manager shall do maintenance and repair of CCI material.

8.4.2.3 Custody of Other COMSEC Materials

MSC defines other COMSEC material as paper based keying material and classified CMS documentation. It must remain under the cognizance of the personnel identified in the EKMS management hierarchy. Paper keying material includes keylists, keying material, code, authenticators (including IFF), one-time tapes and onetime pads. Keying material can be designated for use as operational, exercise, test, maintenance or training.

8.4.3 COMSEC Records

8.4.3.1 Accounting Policy

It is the policy of MSC to simplify, to the maximum extent prudent, the records required at the Secondary Tier 3 LE Holder.

8.4.3.2 Inventory Requirements

When EKMS material is issued to a Tier 3 LE user, it is the responsibility of the LE Holder to ensure the material is placed on a daily or watch-to-watch inventory.

8.4.3.3 Reports Requirements

It is the policy of MSC to reduce required reports made by Tier 3 LEs to a minimum. These minimum reports are detailed in Section 8.5.3.4, Reports Submission.

8.4.4 Safeguarding Equipment and Keying Material

8.4.4.1 Physical Security

It is the policy of MSC that COMSEC material, keying material marked CRYPTO, CCI material and equipment both keyed and un-keyed must be given special command attention to ensure that it is afforded the appropriate security based on type and classification.

8.4.4.2 Storing Requirements

It is the policy of MSC to require CMS material not under the personal control or observation of an appropriately cleared person to be guarded or stored in a GSA-approved security container, vault, modular vault or secure room with an electronic combination lock. If these storage requirements cannot be met promptly afloat, guidance from the EKMS Manager must be obtained.

8.4.4.3 Two-Person Integrity Requirements

For ships with circuits and terminal equipment cleared for Top Secret, the Two-Person Integrity (TPI) requirements will be strictly complied with.

8.4.4.4 Receiving

All receiving Tier 3 LEs are responsible for inspecting all material for evidence of tampering and must make page checks, where required, for completeness.

8.4.4.5 Transferring

Normally, Tier 3 EKMS LEs will not issue any CMS material to any person outside their own command without written authorization from the Primary Tier 3 EKMS Account Manager. In emergency conditions, Primary Tier 3 LE Holders and in special circumstances, Secondary Tier 3 LE Holders may be authorized by the COMSC EKMS Account Manager to distribute CMS material to MSC activities within their respective AORs. This emergency distribution is defined as an “Emergency Modification” and the procedures are detailed in Section 8.5.4.5, Transferring CMS Material.

8.4.4.6 Destruction

Once CMS material is issued to LE Managers and Holders, they are responsible for the complete destruction of all superseded CMS material held. LEs must submit destruction reports to the Primary Tier 3 EKMS Manager as soon as possible but not later than the third working day of the month following the month in which destruction was held. Destruction will be performed by a minimum of two properly cleared individuals.

8.4.4.7 Loss of CMS Material

In the event of loss of any CMS material, prompt action must be undertaken utilizing the procedures outlined in Section 8.5.4.7, Action in the Event of CMS Material Loss. If the COMSEC material cannot be located within a reasonable time, not to exceed 24 hours, the COMSC EKMS Account Manager must be notified utilizing the procedures found in Section 8.5.10, Incident Reporting.

8.4.5 Requirements for Security Clearances and Restrictions on Access to COMSEC Material

8.4.5.1 Security Clearance

The administrative processes based on COMSCINST 5510.8F, COMSC Information and Personnel Security Regulation, must be followed. This clearance plus a need-to-know is the basis for granting access. Access to classified COMSEC material requires a security clearance equal to or higher than the classification of the COMSEC material involved. System administrators and operators for the LMD/KP must be cleared to the highest level of key that they can access, with a minimum clearance level of SECRET. Appointment can be based on an interim security clearance. Access to unclassified COMSEC material does not require a security clearance. Revocation of a security clearance revokes access.

8.4.5.2 Requirement for Access or Need-to-Know

Access to classified COMSEC material must be restricted to properly cleared individuals whose official duties require access to COMSEC material. The fact that an individual has a security clearance and/or holds a certain rank or position, does not, in itself, entitle an individual access to COMSEC material. Access to classified as well as unclassified COMSEC material requires a valid need-to-know and:

- All personnel having access to COMSEC keying material must be authorized in writing by the Commander, Commanding Officer, ship's Master or OIC of an MSC activity. A sample letter of authorization is found in Section 8-9, Sample Forms.
- Knowledge of the combination to the COMSEC vault and safes shall be limited to the Manager, Holders and designated alternate Holders.
- 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 SECNAVINST 5510.30A for the minimum-security education requirements for DON commands.
- Each must execute a User Responsibility form found in Section 8.9, Sample Forms.

8.4.5.3 Military and CIVMAR / Civil Service Personnel

U.S. citizens (includes naturalized) who are U.S. Government employees, or military personnel may be granted access to COMSEC material if they are properly cleared and their duties require access.

8.4.5.4 Contract 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 U.S. contractor personnel to:

- Install, maintain or operate COMSEC equipment for the U.S. Government.
- Participate in the design, planning, production, training, installation, maintenance, operation, logistical support, integration, modification, testing or study of COMSEC material or techniques.
- Electronically communicate classified national security information in a crypt-graphically secure manner or unclassified national security-related information by COMSEC protected means.

8.4.5.5 Foreign Personnel

Foreign nationals will not be granted access to or provided information about COMSEC keying material without written permission from the material's controlling authority.

8.4.6 Training

The MSC EKMS Managers and alternates must meet the training requirements discussed in Section 8.5.6, Training Procedures. The training of users will be tailored to their CMS holdings.

8.4.7 EKMS Primary Tier 3 Manager, Secondary Tier 3 LE Holders and CMS LE User Appointment Criteria

The following criteria must be met when selecting personnel for appointment as Primary Tier 3 EKMS Managers, Secondary Tier 3 Holders and CMS LE Users:

- Must be a U.S. citizen.
- Must have a clearance at the highest level of material held, with a minimum U.S. security clearance – SECRET.
- Must receive CMS User training.
- Must sign a CMS Responsibility Acknowledgement Form.
- Must be designated in writing by the activity's command authority.

8.4.8 Audits

The Primary Tier 2 account is subject to inspection/audit at least once every 24 months. Any or all Tier 3 holdings are subject to review during this inspection. This inspection will be performed on a no-notice basis.

Other inspections/review will be as stated in Section 8.5.8, Audit Procedures. They will include MSC EKMS Account Manager audits of Primary Tier 3 EKMS accounts.

Primary Tier 3 EKMS Managers will conduct periodic audits of Secondary Tier 3 EKMS Holders.

Guidance for audits of Primary Tier 3 EKMS Managers will be provided by the MSC EKMS Manager. Primary Tier 3 EKMS Managers will utilize this guidance in developing their Tier 3 EKMS Holder audits.

8.4.9 Assist Visits

Based on the Primary Tier 3 EKMS Managers assessment of need, Advice and Assist visits should be performed as required. Requests for EKMS Advice and Assist visits will be made to the Primary Tier 3 EKMS Manager. The Primary EKMS Manager and ship/command shall keep a record of assist visits. The MSC EKMS Account Manager shall be advised of any significant results.

8.4.10 COMSEC Incident Reporting

It is the policy of MSC that incident reports are made to the COMSC EKMS Account Manager. The manager will assess the reported circumstances and pass the assessment to the MSC SCMSRO who will report as required to the National COMSEC Incident Reporting and Evaluation System (NCIRES).

Details on NCIRES, types of incidents, and required reports are found in Section 8.5.10, Incident Reporting Procedures.

8.5 MSC EKMS Functions and Procedures

8.5.1 Management Functional Roles and Procedures

8.5.1.1 Staff CMS Responsibility Officer (SCMSRO)

The MSC SCMSRO must be designated, in writing, by the flag officer and have a security clearance equal to or higher than the highest classification of COMSEC material held by the account. The SCMSRO:

- Is responsible for the proper administration of routine matters for MSC's centrally managed EKMS account.
- Is responsible for the proper management and security of all COMSEC material held by his/her command.
- Must ensure compliance with established policy and procedures governing the safeguarding and handling of COMSEC material.
- Must sign COMSEC correspondence and reports as "Staff CMS Responsibility Officer" vice "By direction."
- Will report to COMSC the status of COMSEC posture on a regular basis.
- Will develop policy and procedures for CMS matters within the MSC community.
- Will review training requirements.
- Will submit incident reports in accordance with Section 8.4.10.
- Will appoint EKMS Managers and Alternates.
- Will advise MSC commands regarding CMS and EKMS matters.
- Will conduct unannounced spot checks.

The duties of the SCMSRO cannot be further delegated and must revert to the appointing official in the absence of the assigned SCMSRO.

8.5.1.2 COMSC Account EKMS Manager

The Account Manager is responsible for all actions associated with the receipt, handling, issue, safeguarding, accounting and disposition of COMSEC Material assigned to COMSC's EKMS numbered account. The individual is appointed in writing by the SCMSRO for managing material issued to the account and is directly responsible him/her. The manager is also the primary advisor to the SCMSRO on all matters concerning CMS/EKMS. Duties are that he:

- Acquires, generates, monitors and maintains the command COMSEC material allowance to include an annual review of holdings to verify continued validity of need.
- Maintains proper storage and adequate physical security for LMD/KP suite and all COMSEC material held by the account.
- Always keeps the Alternate Manager(s) informed of the current status of the account.
- Provides LE personnel with written guidance concerning handling, accountability and disposition of issued material.
- Conducts training to ensure all personnel handling COMSEC material are familiar with proper procedures.
- Maintains records/files required by this instruction, CMS21 (current edition) or other competent authority.
- Ensures prompt and accurate submission of account correspondence, messages and accounting reports.
- Issues material to Primary Tier 3 EKMS managers for distribution to assigned Tier 3 LEs.
- Through periodic spot checks, ensures personnel at LEs maintain accountability for material that has been issued to them, including proper inventory and destruction procedures and records.

- Ensures procedures are established to reassign local custody responsibility for COMSEC material held by individuals permanently leaving the command and those departing on TAD/TDY for more than 30 days.
- Ensures all amendments to CMS 21 and all other COMSEC-related publications/ instructions are promptly and correctly entered.
- Maintains the account's portion of the MSC wide Emergency Action Plan (EAP).
- Conducts required inventories and destruction of COMSEC material.
- Ensures proper physical-security measures are maintained when COMSEC material is transported within the command or transmitted outside the command.
- Ensures COMSEC material is properly packaged and shipped via an authorized method.
- Ensures page checks of COMSEC material are conducted as required.
- Ensures TPI requirements are maintained.
- Immediately reports to the SCMSRO any known or suspected insecure practice, Practice Dangerous to Security (PDS) or other CMS Incidents.
- Ensures modifications to COMSEC equipment are performed by qualified individuals and the proper disposal of residue from the modification is made.

8.5.1.3 Alternate EKMS Managers

These mangers are designated in writing, by the MSC SCMSRO to assist the EKMS Manager in the performance of his/her duties and to perform manager duties during the temporary absence of the EKMS Manager. Alternate EKMS Manager(s) share equally with the EKMS Manager for proper management of a COMSEC account.

Duties and responsibilities are identical to those of the EKMS Manager.

- Must always be capable and ready to assume the duties of the EKMS Manager and administer the account in his/her absence.

8.5.1.4 Primary Tier 3 EKMS Manager Responsibilities

The Primary Tier 3 EKMS Manager:

- Consolidates, reviews and monitors of keying material requirements.
- Issues material to LEs and users.
- As directed by the EKMS Manager, conducts periodic spot checks and ensures personnel at LEs maintain accountability for material that has been issued to them including proper inventory and destruction procedures and records.
- Ensures training of personnel to be EKMS LE Holders or users.
- Available to render CMS/EKMS related assistance and support as required.
- Maintains the account's portion of the MSC wide EAP.
- Conducts required inventories and destruction of COMSEC material.
- Maintains copies of Secondary Tier 3 Holders' letters of authorization.
- Ensures proper physical-security measures are maintained when COMSEC material is transported within the command or transmitted outside the command.

- Ensures COMSEC material is properly packaged and shipped via an authorized method.
- Ensures page checks of COMSEC material are conducted as required.
- Ensures TPI requirements are maintained.
- Reports to the SCMSRO via the EKMS Manager, any known or suspected EKMS related incident in their AOR.

8.5.1.5 Secondary Tier 3 EKMS Local Element Command Responsibilities

The Squadron Commander, ship's Master and OIC of mobile units plus the Commander ashore is the LE individual ultimately responsible for the proper administration of the command's COMSEC holdings and compliance with established CMS policy and procedures. Duties include:

- Ensures compliance with established policy and procedures.
- Utilizing appointment criteria found in Section 8.4.8, appoints, in writing, qualified and responsible individuals as EKMS LE Primary and Alternate LE Holders with copy to the Primary EKMS Tier 3 Manager.
- Designates, in writing, a list of personnel authorized access to keying material.
- Ensures training requirements are met.
- Ensures COMSEC related events are promptly submitted and corrective action is taken as required.
- Ensures that EAP is established and tested on a semi-annual basis.
- Ensures an inventory of all COMSEC material held is conducted semiannually or as directed by the EKMS Manager.
- Ensures that the assignment of additional collateral duties to personnel that manage the account will not interfere with their primary responsibilities.

8.5.1.6 Secondary Tier 3 EKMS Local Element Holder Responsibilities

The duties and responsibilities of the LE Holder and Alternates are virtually identical to those of the parent account Manager and Alternates, except for reporting requirements.

The LE Holder and Alternate are responsible for:

- Maintaining required files.
- Ensuring the proper safeguarding, storage, destruction and usage of COMSEC material issued.
- With the exception of the semiannual inventories initiated by the MSC EKMS Manager, performing required reporting and accounting via the Primary Tier 3 EKMS Manager.

8.5.1.7 CMS User Responsibilities and Duties

The users of COMSEC equipment and devices are responsible for the proper operation of this equipment, its safeguarding and ensuring that unauthorized personnel do not have access to this equipment.

8.5.2 Procedures for Handling COMSEC Material

8.5.2.1 General

The ultimate effectiveness and protection provided by COMSEC material, systems, equipment and techniques are dependent upon the actions of each individual user of COMSEC material. All the security achieved through the proper use of cryptographic systems is to a large extent dependent upon the physical protection afforded the associated keying material and those facilities where this material is stored.

Each MSC person involved in the use of COMSEC material is personally responsible for:

- Safeguarding and properly using the material they use or for which they are responsible.
- Promptly reporting to proper authorities any occurrence, circumstance or act which could jeopardize the security of COMSEC material.

The MSC EKMS Manager will issue to Primary Tier 3 EKMS Managers, the CMS material required to support the requirements of assigned Secondary Tier 3 EKMS elements and other local users.

Any reproduction of COMSEC material will be accomplished or approved by the MSC EKMS Account Manager. Reproduction will only be accomplished when time or delivery constraints preclude normal supply of the material.

Issues to LEs. Primary Tier 3 EKMS Managers will direct monthly issues of COMSEC material. LE Holders will make advance arrangements for pick-up, courier or electronic delivery. Emergency delivery may be coordinated through the Primary Tier 3 EKMS Manager on a case-by-case basis. Monthly issues to ships or remote shore facilities will ensure an adequate Reserve On Board (ROB) level is maintained to support required operational readiness.

8.5.2.2 Use of Over-the-Air Distribution (OTAD) for COMSEC Key Material

To the maximum extent feasible MSC will distribute Traffic Encryption Key (TEK) via OTAD. For MSC users who do not have OTAT service available via the Fleet Broadcast, the MSC EKMS Manager will load or generate keying material via KOK 22 and transfer to Primary Tier 3 Manager. When appropriate and if transfer directly to a Secondary Tier 3 user is required, it will be accomplished using STU III/STE and DTDs.

The COMSEC Material Control System is not involved in accounting for electronic keys that are converted from tape for OTAD or are field generated. Therefore, MSC becomes the Controlling Authority (CA) of key generated and is responsible for identifying and tracking it.

Stations that transmit, relay or receive key via OTAT must maintain local records, to verify that intended delivery has been accomplished. These records should utilize the form found in Section 8.9, Sample Forms. Local records should retained for 6 months beyond the duration of the effective cryptographic period of the key.

8.5.2.3 Custody of Controlled Cryptographic Items (CCI)

MSC utilizes the personnel in the EKMS management hierarchy to be holders of Cryptographic Controlled Items (CCI). Distribution and return as well as maintenance and repair of CCI will be done within the MSC EKMS management structure. Maintenance and repair of CCI shall be done by certified shore activities designated by the MSC EKMS Manager.

A security clearance is not required for access to un-keyed CCI. Normally, access must be restricted to U.S. citizens whose duties require such access.

Un-keyed 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. 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 chapter.

8.5.2.4 Custody of Other COMSEC Material

MSC defines other COMSEC material as paper based keying material and classified CMS documentation. It must remain under the cognizance of the personnel identified in the EKMS management hierarchy. Paper keying material includes keylists, keying material, code, authenticators (including IFF), one time tapes and onetime pads. Keying material can be designated for use as operational, exercise, test, maintenance or training.

The process for maintaining paper material is as follows:

- The Tier 2 MSC EKMS Manager will maintain all paper key lists as required in CLF/CPF C2281.1 (series).
- Tier 3 and users will only be issued paper keying material that is actually used by the units.
- Area sensitive paper key material will be held by the area Primary Tier 3 EKMS Managers.

8.5.3 COMSEC Records

8.5.3.1 General Information

All COMSEC material accounting is based on a calendar year cycle. COMSEC Material Accounting Reports (SF 153) provide an audit trail for each item of accountable COMSEC material. These reports include:

- Transfer
- Destruction
- Receipt
- Inventory

One-Time Keying Material Destruction Report Form CMS 25 is utilized for local recording of keytape segments.

Samples of both forms are found in Section 8.9, Sample Forms.

8.5.3.2 Accounting Practices

For record keeping purposes, LE Managers and Holders will:

- Maintain a locally prepared watch-to-watch inventory of material held.
- Maintain folder for receipts for material held.
- Maintain folder for all transferred material.
- Maintain folder for all destroyed material.
- Maintain folder of communications regarding CMS material holdings (i.e., naval messages, faxes).
- Keep an OTAT log.

Procedures require that material is to be referred to by short title and serial number and that records be kept for 2 years.

Sample forms are found in Section 8.9, Sample Forms.

8.5.3.3 Inventory Procedures

When EKMS material is issued to a LE, it is the responsibility of the LEs Holder to ensure the material is placed on a daily or watch-to-watch inventory. Locally prepared inventory forms may be used. Sample forms are found in Section 8.9, Sample Forms, found below.

While on duty, each watch supervisor is responsible for all COMSEC material listed on the watch-to-watch inventory, regardless of which watch supervisor signed the local custody document for the material.

Each time the watch changes, or each time the watch is assumed, the oncoming watch supervisor must inventory all keying material, publications and COMSEC equipment held by the watch station.

A progressive inventory listing of all keying material, publications and equipment held by the watch station must be maintained.

Material must be listed by short title, edition, accountability legend code and accounting number (if any). As the watch station receives new material, it must be added to the inventory; as material is destroyed or returned to the holder, it must be deleted from the inventory. All paper keying material will be inventoried by sighting its short title, edition, accounting number and sequence number of the exposed segment. Equipment may be inventoried by quantity only. Watch station personnel must ensure all key tapes (loose segments) held by the watch are placed on the progressive inventory until superseded.

The progressive inventory must be designed to provide a means of recording dates and initials or signatures to certify that the inventory was conducted. Superseded progressive inventory listings must be retained for 30 days.

All unsealed keying material (except keying material packaged in canisters) held by the watch station must be page-checked.

For keying material canisters:

- Verify the segment number of the visible segment to ensure it matches the inventory.
- If the detached segment is Top Secret, the key tape segment that may have been unintentionally removed from its canister before its effective period must remain under TPI and be sealed in an envelope.
- Each keytape segment that cannot be destroyed immediately after use because it is still effective and it is TS, must remain under TPI. It must be carefully stored and accounted for. This includes each last copy of a multiple-copy key segment that was removed from its canister and is being held until superseded.
- Destruction of key tape segments is to be documented on Form CMS-25A found in Section 8.9.6.

Superseded extracts of all keying material destroyed must be confirmed by sighting the appropriate local destruction records. Page checks must be recorded either on the material itself, on the progressive inventory, or by any other means, which will verify that each required page check is performed.

Any inventory discrepancies discovered during the watch inventory or when conducting required page checks must be reported immediately to the LE Holder.

8.5.3.4 Reports Submission

The COMSC EKMS Manager is responsible for all CMS reports required by NSA, DoD and DON. To support timely submission of reports to higher authority, the Tier 2 EKMS Manager requires the Tier 3 EKMS Managers and Holders to submit their inputs as follows:

- Inventory Reports. These reports will be completed on SF 153 and shall be submitted to the EKMS Manager on a semiannual basis for all material held. Reports are due by 15 December and 15 June. Secondary Tier 3 EKMS Holders shall copy their Primary Tier 3 Managers on this report.
- Receipt Reports. Completed SF 153 Receipt reports will be submitted within 3 working days to the EKMS Manager. Secondary Tier 3 Managers will copy their Primary Tier 3 Managers on this report.
- Destruction Reports. Upon verification of the complete destruction of local records, the Primary Tier 3 EKMS Manager and the Secondary Tier 3 EKMS Holder will submit a destruction report to the EKMS Manager. This report must be made no later than the third working day of each month.

NOTE: LEs at sea are authorized to submit monthly destruction reports via record message traffic. Ensure message traffic destruction reports contain all necessary accounting data for the material destroyed. Copies of all destruction reports held by the LE will be maintained for 90 days.

8.5.4 Safeguarding Equipment and CMS Holdings

8.5.4.1 Physical Security

CCI equipment that is unclassified and un-keyed will be given protection equivalent to that of high value government equipment. Precautions will be taken against theft and sabotage.

Keyed CCI equipment must be protected equivalent to the level of key. No access is to be given by unauthorized personnel, persons without proper security clearance or a need to know. Physical protection must prevent ease of removal of components from storage location.

8.5.4.2 Storing

The EKMS Managers, Holders and users are responsible for ensuring the safe storage and positive control of all CMS material within the command following the policy set forth in Section 8.4.4.2. Inspections and spot checks will be conducted to ensure that proper physical security and control is provided.

- SECRET and CONFIDENTIAL keying material will be stored in a GSA approved field safe or security container secured by a GSA approved electronic locking device.

- For each locking mechanism, two copies of SF 700 will be placed inside the safe or vault with a copy stored in another designated secure place. An SF 702 will be used to record opening, closing and checks for each lock.
- Combinations of containers used to store CMS distributed material shall be changed:
  - Whenever a person having knowledge of the combination is transferred from the command or no longer requires access.
  - Whenever the combination becomes known or is suspected to have become known to an unauthorized person.
- Annually.
- When placed in use after procurement.
- When taken out of service.

8.5.4.3 Two-Person Integrity (TPI)

TPI is a system of handling and storing designed to prevent single-person access to certain COMSEC material identified below.

- 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 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 must be applied to the following COMSEC material from time of receipt through issue to LEs or destruction:
  - All TOP SECRET paper keying material marked or designated CRYPTO.
  - Fill Devices (FDs) or other physical media (floppy disks, magnetic tapes, etc.) storing unencrypted TOP SECRET key.
  - Equipment containing TOP SECRET key that allows for key extraction.
- Access to and knowledge of combinations protecting TPI material at all MSC EKMS Manager levels must be restricted to only the EKMS Manager and Alternate(s). No one person will have access to or knowledge of both "A" and "B" combinations to any one TPI container/safe.
- All TOP SECRET COMSEC material evolutions (e.g., generation, OTAT, transfer, receipt and issue to LEs, destruction) must be conducted by two properly cleared persons.
- After a container holding TPI material 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.

At the LE level, TPI must be applied to the following COMSEC material from time of receipt through turn-in to the MSC EKMS Manager or Alternate, or destruction:

- All TOP SECRET paper keying material marked or designated CRYPTO.

- TOP SECRET electronic key whenever it is generated, transferred (OTAR/OTAT), relayed or received (OTAT) in an unencrypted form. There are no TPI requirements for recipients of key received via OTAR under conditions where no FD is required at the receiving terminal.
- FDs containing unencrypted TOP SECRET key.
- Unloaded FDs in an operational communications environment containing keyed crypto-equipment from which unencrypted TOP SECRET key may be extracted.
- Equipment which generates and allows for the extraction of unencrypted TOP SECRET key.

At the Local Element Level**:**

- Two authorized persons must be present and remain within sight of each other and the TPI material whenever it is accessed and handled. For example:
  - Removing unencrypted TOP SECRET key marked or designated CRYPTO from COMSEC equipment (to include key variable generators (e.g., KG-83)).
  - TPI is not required at any level for COMSEC keying material marked SECRET, CONFIDENTIAL or UNCLASSIFIED, regardless of CRYPTO markings.

8.5.4.4 Receiving CMS Material

Upon receipt, LE Holders must do the following:

- Inspect all material for evidence of tampering.
- Page check for completeness, where appropriate.
- Verify the short title, edition and serial number with the enclosed SF 153.
- Verify for all key tape canisters that the visible segment is segment 1. If not, notify the EKMS Manager immediately.
- Complete the SF 153 and send it to the Primary Tier 3 EKMS Manager.
- Tier 3 holders will apply status markings, as appropriate.

NOTE: For keying material, obtain the effective CRYPTO period from EKMS Manager or Source Inventory Control Point (ICP) Manager as appropriate. This must be done via secure means; i.e., voice call on STU III, classified message or over the SIPRNET.

8.5.4.5 Transferring CMS Material

EKMS LEs will not normally transfer or issue any CMS material to any person outside their own command. However, equipment malfunctions, operational events, and other unforeseen circumstances may require the "Emergency" transfer of CMS material between Secondary Tier 3 Holders. This cannot be done without approval of the Primary EKMS Manager. The following guidance is provided:

- Prior to any transfer, obtain the express authorization from the COMSC EKMS Manager via Naval Message or secure voice.

- Prepare an SF 153, Transfer Report. Identify short title, edition, quantity and accounting number of material being transferred. Place the original SF 153 and one copy in an envelope and send with the package. Reference the approval authority on a retained copy.
- Package and send the CMS material as directed by the EKMS Manager. Classified material must be sent in a double-wrapped and properly-marked package.
- If any loose keymat segments are sent, package the segment in a sealed envelope within the package and ensure it is recorded on the SF 153.

8.5.4.6 Destroying CMS Material

Once CMS material is issued to LE Holders, they are responsible for the complete destruction of all superseded CMS material held. LEs must submit destruction reports to the EKMS Manager by the third working day of the following month in which destruction was held. Destruction will be performed by a minimum of two properly cleared individuals. The following procedures will be observed:

- The material to be destroyed will be separated from all other similar material. Material to be retained will be removed from the general area in which destruction will take place.
- The material to be destroyed will be arranged in the same order as it appears on the corresponding local destruction record (SF-153 or equivalent).
- The person responsible for conducting the destruction shall read each short title, edition suffix (if any) and accounting number to the witness who will mark the appropriate entries on the destruction record. Prior to destruction of a canister all markings will be removed. To prelude inadvertent or unauthorized destruction of the material, care shall be taken to ensure that pages are not stuck together.
- In turn, the witness will read each short title, edition, suffix (if any) and accounting number to the person responsible for conducting the destruction who will make the appropriate entries on the destruction record.
- Immediately after verifying the accuracy and completeness of the line entries, one person will insert the material into the destruction device while the other person observes as a witness. Once issued, individual segments of unsealed extractable key list and keycards must be destroyed immediately when superseded. If immediate destruction is not possible, the superseded segments may be retained up to, but no longer than 12 hours, after their being superceded. The CMS-25 Form or equivalent must be used as a local destruction record.
    - Destruction of electronic key material held in the DTD will be destroyed as above.
    - Superseded-keying material not immediately destroyed will be stored in a container under TPI.
    - Emergency supercession of keying material marked "CRYPTO" is directed by Joint ICP manager or general messages addressed to ALCOM, ALCOMLANT, ALCOMLANT ALFA or ALCOMPAC PAPA. Upon receipt of an emergency suppression, destroy material as directed and arrange for replacement material from the EKMS Manager, if necessary.

8.5.4.7 Action in the Event of Loss of CMS Material

In the event of loss (or suspected loss) of keying material:

- Stop all procedures immediately.
- Search entire area.
- Recheck all keying material which has been used and the remaining keying material in the card book or key list.
- If the material cannot be located, follow the procedures contained in Section 8.5.10, COMSEC Incident Reporting.

8.5.5 Procedures for Acquiring and Reporting Personal Security Clearances and Restricting Access to COMSEC Material

Personnel Security Clearances for all categories of personnel performing functions requiring access to classified information or equipment are to be processed as detailed in COMSCINST 5510.8F, COMSC Information and Personnel Security Regulation. This clearance must be completed before any access to COMSEC keying material can take place. Access to COMSEC keying material must be authorized in writing by the Commanding Officer. An individual letter or an access list may be used for this authorization.

- If an individual letter is used, the letter remains in effect until the status for an individual changes (i.e., a change in clearance status or duties no longer require access to COMSEC keying material).
- If an access list is used, it must be updated whenever the status of an individual changes or at least annually.
- Knowledge of combination to safes containing CMS distributed material held by CMS users will be limited to personnel authorized in writing by the Commanding Officer.

8.5.5.1 Military and CIVMAR / Civil Service

SECNAVINST 5510.30A, DON Personnel Security Program, under the authority of Executive Order (E.O.) 12960, addresses access to classified information, security requirements for government employees and contract personnel. The objective of the Personnel Security Program is to authorize in continued access to classified information and/or initial and continued assignment to loyalty, reliability and trustworthiness are such that entrusting the persons with classified information or assigning the persons to sensitive duties is clearly consistent with the interests of National security. Additionally, the Personnel Security Program ensures that no final unfavorable personnel security determination will be made without compliance with all procedural requirements.

8.5.5.2 Contractor and Foreign

The SCMSRO must authorize transfers to contractor and foreign CMS accounts. Before releasing COMSEC material to a contractor account, the provisions of OPNAVINST 2221.5B, Subj: Release of COMSEC Material to U.S. Industrial Firms under Contract to the U.S. Navy, must be met.

In the event that a project/contracting officer has not fulfilled the requirements of OPNAVINST 2221.5B, prior to the release of COMSEC material to a contractor account, the SCMSRO must obtain permission must be obtained from DCMS//30// by submitting the following information:

- Identity of Navy project office/contracting office.
- Contractor's name and address.
- Contract number.
- Identity of COMSEC material involved.
- Any other information deemed appropriate in evaluating the request.

8.5.6 Training Requirements and Sources

8.5.6.1 Tier 2 EKMS Manager and Alternate

The Tier 2 EKMS manager and at least one alternate must attend the formal EKMS Manager COI provided by area Fleet Training Centers.

8.5.6.2 Primary Tier 3 EKMS Manager and Alternate

The Tier 3 EKMS Managers and at least one alternate must attend the formal EKMS Manager COI provided by area Fleet Training Centers.

8.5.6.3 Secondary Tier 3 Holders and Users

All Secondary Tier 3 Holders will attend a COI on the Operation, Administration and Handling of COMSEC material. A 3-day COI will be taught once a month at a location to be specified by the COMSC EKMS Account Manager and as needed upon request from individual units. The course will be at no cost to units in the local area. For units out of area, the cost will be travel and per diem either to have the instructor come to them or for their travel to one of the training sites.

All CMS users will complete the COMSEC users Computer Based Training (CBT), within 1 month after being assigned as a CMS user.

8.5.7 Procedures for EKMS Holder and CMS User Appointment

Following the appointment criteria found in Section 8.4.7, procedures for completion of the appointment of EKMS Holders and CMS users include:

- Completing the required training.
- Being designated in writing by the activity's command authority.
- Signing a CMS Responsibility Acknowledgement Form as found in Section 8.9, Sample Forms.
- Attending monthly procedure reviews as directed.

8.5.8 Audit Schedules and Procedures

An audit of all EKMS elements should be held in conjunction with TYCOM Inspections. This includes review of Primary Tier 3s when appropriate. Sample checklists may be obtained from the MSC EKMS Manager for Audit of Primary Tier 3 EKMS Managers and for Primary Tier 3 EKMS Managers review of Secondary Tier 3 activities.

8.5.9 Assist Visit Requests and Coordination

Ships/commands requiring an assist visit shall make requests via the COMSC EKMS Account Manager who will initiate a formal request to a local CMS Advise and Assist Team in the area of the unit making the request.

8.5.10 COMSEC Incident Reporting

8.5.10.1 General

A COMSEC incident is any actual or suspected loss or compromise of CMS distributed material as described below. Such incidents shall be reported immediately to the COMSC EKMS Account Manager. The EKMS Account Manager will assume control over any COMSEC incident reporting outside the MSC claimancy.

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 posed to secure communications by COMSEC material mishandling, losses or thefts, the NSA established the National COMSEC Incident Reporting and Evaluation System (NCIRES).

COMSEC incidents are divided into three categories; Cryptographic, Personnel and Physical. Incidents may be unique to a given crypto system, or to an application of a crypto system. Reportable incidents specific to the Data Transfer Device (DTD) are found in Section 8.8, DTD Policies and Procedures.

8.5.10.2 Types of Incident Reporting

There are four types of incident reports: initial, amplifying, final and interim cryptographic incidents. Examples of cryptographic incidents are:

- Use of COMSEC keying material that is compromised, superseded, defective, previously used (and not authorized for reuse) or incorrect application of keying material.
- Discussion via non-secure telecommunications of the specific details of a COMSEC equipment failure or malfunction.
- Detection of malicious codes (VIRUSES) on the EKMS system (LMD/KP).
- Any other occurrence that may jeopardize the cryptographic security of a COMSEC system, such as:
  - Use of any keying material for other than its intended purpose.
  - Unauthorized extension of a crypto period.
  - Any other occurrence that may jeopardize the crypto-security of a COMSEC system.

8.5.10.3 Personnel Incidents

Examples of personnel incidents are:

- Known or suspected defection.
- Known or suspected espionage.
- Capture by an enemy of persons who have detailed knowledge of cryptographic logic or access to keying material.
- Unauthorized disclosure of Personal Identification Numbers (PINs) and/or passwords that are used on systems which also allow access to COMSEC material/information.
- Attempts by unauthorized persons to effect disclosure of information concerning COMSEC material.

8.5.10.4 Physical Incidents

Examples of physical incidents are:

- The physical loss of COMSEC material. This includes whole editions as well as a classified portion thereof.
- The loss or compromise of KP CIKs and non-zeroized KP KSDs-64As, KP keys (EKMS FIREFLY and EKMS MSK), floppy disks containing key or other EKMS information or KP PINS.
- Unauthorized access to COMSEC material by persons inappropriately cleared or not cleared.
- COMSEC material discovered outside of required accountability or physical control or COMSEC material improperly packaged or shipped.
- Material reported destroyed but not destroyed.
- Material left unsecured and unattended.
- Failure to maintain TPI.
- CMS material improperly packaged or shipped.
- Material received with a damaged inner wrapper.
- Destruction by other than authorized means.
- Material not completely destroyed and left unattended.

- Unauthorized maintenance.
- Known of suspected tampering with or unauthorized modification to COMSEC equipment.
- Unauthorized copying reproduction or photographing.
- Deliberate falsification of records.
- Any other incident that may jeopardize the physical security of CMS material.

8.5.10.5 Incident Procedures

Actions to be taken in any incident include the following:

- Contain, isolate and secure CMS material to prevent further compromise or loss of security.
- Gather information regarding the event.
- Record names of all personnel involved.
- Identify material involved.
- Minimize further risk.
- Prepare report utilizing proper classification in reporting.

8.5.10.6 Incident Reports

The initial report will be submitted to the COMSC EKMS Account Manager. The Manager will determine the requirements for amplifying, final and interim reports together with the required guidance. This Initial Report will be submitted by IMMEDIATE precedence classified message or secure phone call. Classify the incident reports according to content of the message or letter text. Incident messages concerning unclassified DES key will be classified UNCLAS EFTO. All other incident messages should be classified a minimum of CONFIDENTIAL. This report will include:

- Subject
- References
- Material involved
- Personnel involved
- Circumstances of incident
- Command compromise assessment on incident

8.6 Emergency Action Plan

Manager/Holder of CMS material and the Command Security Manager shall ensure that a detailed EAP for all classified material is prepared and updated periodically. All hands will thoroughly familiarize themselves with the provisions of the EAP. All LEs are responsible for preparing their own EAP to fit the needs of their command. Emergency destruction plans for CMS material is not required for shore commands within CONUS; however, proper safeguards for CMS distributed material are required during natural disasters and terrorist threats. All LEs, ships and shore stations outside of the continental United States must maintain an emergency destruction plan.

8.7 Policies and Procedures for Secure Telephone Unit III (STU III) and Secure Terminal Equipment (STE)

8.7.1 Background

The STU III and its replacement STE are in use throughout MSC for secure voice and messaging services. More than half of all MSC Secondary Tier 3 EKMS Holders have a STU III as their only cryptographic device. Over four hundred STU IIIs and a growing number of STEs are in use supporting both ashore and afloat users. The STU III has limited data handling capabilities and is being replaced with the more capable STE. Key support for the STU III will be limited after 2005.

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 KOV-14 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 its predecessor the STU-III. In addition, the STE offers advanced features such as secure voice conferencing and fast auto-secure negotiation with other STEs on ISDN services. When a STE is connected to an STU-III on the analog telephone network, the STE will emulate an STU-III. 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 MSE or TRI-TAC switches. With the addition of the optional Future Narrow Band Digital Transmission (FNBDT) protocol, the STE will be able to negotiate secure sessions with future digital wireless handsets and other FNBDT products.

8.7.1.1 The STU III

The equipment, as long as it is un-keyed, can be handled as a valuable component but must be accounted for as CCI.

The Key Storage Device or KSD-64 is the physical device that can be used as a FD and also as a Crypto Ignition Key (CIK). It is a small device shaped like a physical key and contains passive memory.

When designated a CIK, this device is used to protect key that has been downloaded into COMSEC equipment. The CIK contains an electronic "password" that is used to electronically lock and unlock a terminal's secure mode. The secure mode is unlocked when the CIK is inserted and turned, and locked when the CIK is removed.

FD is an unused Key Storage Device (KSD-64A) used to carry keying material to a STU-III terminal FDs are produced and distributed by the EKMS CF.

User CIK is a Key Storage Device or KSD-64A is used to lock and unlock the secure mode of the terminal with which it is associated. Additional CIKs may not be created from a User CIK.

These are controlled devices and their Crypto Ignition Keys are distributed through EKMS.

8.7.1.2 The STE

The STE is a high dollar-value sensitive, pilferable item; therefore, DoD and Navy logistics, property accounting and security controls must be strictly adhered to.

8.7.1.3 KOV-14 Fortezza

The KOV-14 card is assigned Accounting Legend Code 1 (ALC-1). This means that the KOV-14 card must be accounted for within the CMCS by its unique serial number, not the keying material identification number on the tags, until the card is physically destroyed. The KOV-14 card can only be procured, installed and operated by U.S. Government departments or agencies and their contractors who have a COMSEC account.

A KOV-14 card may be a fill, user, carry, TPA or UN-keyed (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.

A fill card is a keyed KOV-14 card that has not been associated with a STE. A fill card may be programmed with seed, test or operational keying material and accountable to the COMSEC Account's COR. A COMSEC Holder or TPA 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 a STE.

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.

8.7.2 MSC Policy

8.7.2.1 Management

STU III and STE equipment custody will be handled and accounted for as CCI under the centralized direction of the MSC EKMS Account Manager as set forth in Section 8.4.2.2. MSC Primary Tier 3 EKMS Managers may be assigned specific supporting tasks as required.

Key Storage Device KSD-64 and KOV-14 Fortezza Plus card are cryptographic elements with custody and handling under the direction of the MSC EKMS Manager as set forth in Section 8.4.2.3. MSC Primary Tier 3 EKMS Managers may be assigned specific supporting tasks as required.

In transitioning to STE capabilities, priority will be given to ship-shore circuits as identified and coordinated by MSC N6.

Subject to approval by the SCSRMO, the MSC EKMS Account Manager will be responsible for development of any Standard Operating Procedures (SOP) for STU III and STE end users required to supplement the operating manuals provided with the issued equipment.

8.7.2.2 Handling

Handling will be in accordance with Section 8.4.2.2, Custody of Controlled COMSEC Material.

8.7.2.3 Records

The required COMSEC records are as identified in Section 8.4.3. In addition, Command User Lists containing a current record of the holder name, equipment ID and physical location of each item will be maintained at each LE.

A current file of User Acknowledgement Forms will be maintained. A sample form is found in Section 8.9, Sample Forms.

8.7.2.4 Safeguarding

In addition to the Safeguarding Equipment and Keying material requirements identified in Section 8.4.4:

- FDs must be securely stored in accordance with its converted classification.
- CIKs must be protected against unauthorized access and use.
- A user who accepts the use of a KOV-14 card is solely responsible for safeguarding the card.
- When inserted in a STE, the KOV-14/STE system is classified and must be protected to the highest security level that the KOV-14/STE can achieve.
- An authorized person must supervise access by a person not having an appropriate clearance to a STE with an inserted KOV-14.

8.7.3 MSC Procedures

Detailed procedures are contained in equipment operation handbooks and separate SOPs may be provided as required for both the STU III/KSD-64 and the STE/KOV-14.

8.7.3.1 Management

The MSC management structure administration and control for STU III/STE CCI parallels that described in Section 8.5.1, Management Functional Roles and Procedures.

Tier 3 EKMS Managers and Holders will be responsible for the upkeep, initial keying and re-keying of all STU-III phones. This also includes conducting an inventory of all STU-III phones periodically and when requested by the MSC EKMS Manager, i.e., Change of Command, Change of SCMSRO, Fixed Cycle Inventory or Change of Holder.

8.7.3.2 Handling

STU-III telephone accountability is maintained in the EKMS system, whereas the STU-III keys are not. STU-III Key "User Representative" privileges are authorized by COMSC. User Representatives have the authority to order STU-III keys directly from the STU-III section of the CF. All LEs must submit request to EKMS Manager/User Representative for key ordering. LEs must manage their own stock of STU-III keys onboard to support operations.

If it becomes necessary to transport a keyed STU-III from one location to another, the CIK must not be left inserted in the STU-III or in the transportation container.

8.7.3.3 Record Keeping

Each individual who requires issue of STU III materials on local custody will execute a COMSEC Material Responsibility Acknowledgement Form and then return it to the Tier 3 Manager or Holder for retention. A copy of this form is found in Section 8.9, Sample Forms.

The KOV-14 card is assigned ALC-1. This means the KOV-14 card must be accounted for within the MSC CMCS under the MSC EKMS Manager.

8.7.3.4 Safeguarding

Store FDs in accordance with their converted classification per Section 8.5.4.2.

Protect CIK against unauthorized access and use.

Master CIKs allow for the creation of additional CIKs and warrant additional protection. They must be securely stored in accordance with the classification of the key with which they are associated.

A User who accepts the use of a KOV-14 card is solely responsible for safeguarding the card and cannot further transfer the card without the knowledge of the MSC EKMS Manager. A User may allow or permit other people to use his 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 can be transported without written courier authorization.

When inserted in a STE, the KOV-14/STE system is classified and must be protected to the highest security level that the KOV-14/STE can achieve and must meet the criteria of Section 8.5.4.2.

An authorized person must supervise access by a person not having an appropriate clearance to a STE with an inserted KOV-14.

When operationally required, authorized personnel may permit others not normally authorized, e.g., persons whose clearance does not meet the level indicated on the display and foreign nationals, to use the keyed terminal under the following conditions:

- The call should be placed by an authorized person (foreign nationals use should be in the continuous presence of an authorized person).
- After reaching the called party, the caller should identify the party on whose behalf the call is being made, indicating their level of clearance.

8.8 Policies and Procedures for Use of the Data Transfer Devices (DTD*)*

8.8.1 Background

As described in Section 8.3.2, MSC's EKMS Concept of Operations, and shown in Figure 8-1, MSC CONOPS for Tier 2 Support to Tier 3 LEs, the DTD is a key element in EKMS implementation. It provides a primary enabler for the EKMS Manager and Primary Tier 3 EKMS Managers to transfer keying material to Secondary Tier 3 Afloat and Mobile LEs.

The AN/CYZ-10 Data Transfer Device is a small light weight, electronically programmable COMSEC FD which performs key loading, storage and transfer functions currently performed by electronic Common Fill Devices (CFDs, KYK-13 and KYX-15). The DTD comprises five functional areas that interact to effect KEYMAT receipt, storage, transfer and destruction. The device is capable of storing up to 1,000 128-bit keys. As an integral part of the EKMS, the DTD was designed to eliminate the dependency on these system unique storage/loading devices, and hard copy fill requirements. 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) for special functions. The COMSEC side performs the cryptographic functions.

The DTD uses a CIK to control access to the cryptographic capabilities of the device. The CIK, when inserted, generates local Key Encryption Key (LKEK) for combination with resident key material to provide individualized supervisor/user accessibility. Designated Supervisor CIKs provide access to all DTD functions while User CIKs have limited capability. The CIK by itself is unclassified, accountable for locally.

The DTD is classified by a combination of two factors. One is the classification of the key that is accessible when the CIK is inserted, and the second is the highest level of classified data (if any), contained on the host side of the DTD. With the CIK removed and no classified data present on the host side of the DTD, the device is unclassified, CCI. When a valid CIK is inserted, the DTD assumes either the security classification associated with the highest classification level of the KEYMAT it contains, or the highest classification level of information present on the host side, whichever is higher.

8.8.2 DTD Use Policy

Under the direction of the MSC EKMS Manager, DTD equipment will be issued to all Primary Tier 3 EKMS Managers and Secondary Afloat and Mobile Tier 3 LEs.

CIKs will be stored separately from the associated DTD to prevent unauthorized access.

Simultaneous access to a CIK and its associated DTD must be restricted to persons cleared to the highest level of data on the host side, as well as to the highest level of key that can be extracted in unencrypted form by that CIK.

Handling and safeguarding records shall comply with the criteria set forth in Sections 8.4.2, 8.4.3 and 8.4.4.

8.8.3 Procedures

When the CIK is removed and no classified data present on the host side of the DTD, the device is unclassified, CCI and is handled as described in Section 8.5.2.3, Custody of CCI.

When a valid CIK is inserted, the DTD assumes either the security classification associated with the highest classification level of the KEYMAT it contains, or the highest classification level of information present on the host side, whichever is higher and is handled as described in Section 8.5.2.1.

When either the KEYMAT or Host side classification is Top Secret, it requires protection under existing TPI instructions described in Section 8.5.4.3, Two-Person Integrity.

When authorized users will not be present, a Top Secret CIK must be removed from the DTD and returned to TPI storage.

Emergency destruction requires zeroizing the DTD and physical destruction of the unit.

8.9 Sample Forms

Sample forms, both blank and filled out examples, are provided by separate CD distributed by the MSC EKMS Manager. Selected forms with typical data entries are also provided below.

8.9.1 Holders and Users Appointment

Refer to Sections 8.4.7 and 8.5.7, EKMS.

SAMPLE
COMMUNICATIONS SECURITY (COMSEC) MATERIAL SYSTEM (CMS)/ ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS) LETTER OF APPOINTMENT

Date: _____

From: Commanding Officer/Master of _____
To: _____

Subj: COMMUNICATIONS SECURITY (COMSEC) MATERIAL SYSTEM (CMS)/ ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS) LETTER OF APPOINTMENT

Ref: (a) COMSCINST 2000.2, Chapter 8

Encl: (1) Responsibility Acknowledgement Form

1. In accordance with reference (a), Sections 8.4.7, Appointment Criteria, and Section 8.5.7 Procedures for EKMS Managers, Holders and CMS Users, you are hereby appointed as CMS/ EKMS Tier Primary [or Alternate] Tier 3 Manager [or] [Secondary CMS/EKMS User] for this command.

2. LE account number: _____.

3. Certification date for the CMS COI [V-4C-0014 or V-4C-0031] completion date is: [YYMMDD].

4. Security clearance: [TOP SECRET, SECRET, etc, as applicable].

5. The following designation requirements specified in reference (a) are waived:

a. _____
b. _____
(identify authority for and specific requirement(s) waived; if no requirements waived, indicate "None")

6. You must be familiar with reference (a) and must execute the appropriate User Responsibility Acknowledgement form provided as enclosure (1).

(Signature of Commanding Officer/Master)
(Name of Ship)

8.9.2 User Responsibility Acknowledgement

Refer to Sections 8.4.5 and 8.5.7, EKMS. There are two sample Acknowledgement Forms provided on the following pages:

- The first is for a CIVMAR ship user with a wide range of installed cryptographic equipment.
- The second is for a ship with a PC –to-PC Transfer System (PPTS) or an MSC office user that will have only an STU/STE. This second acknowledgement form provides some specific guidance regarding the handling of crypto-related elements and function and reduces user dependence on this chapter.

Commands and activities holding only STU/STE equipment will utilize "User Responsibility Acknowledgement Form B;" all others will utilize Form A. The original of a completed form will be forwarded to the MSC EKMS Manager and a copy to the Tier 3 Primary EKMS Manager. Copies will be retained by the originating command in the appropriate file for 2 years after the individual has been relieved of CMS related duties.

Form A:

CMS RESPONSIBILITY ACKNOWLEDGMENT - Multiple CMS Material

FROM: _____
(RANK/RATE, Full Name, SSN and Command of CMS User)

TO: MSC CMS HOLDER / EKMS Manager Account (local)

SUBJ: CMS RESPONSIBILITY ACKNOWLEDGMENT

REF: (a) COMSCINST 2000.2

1. I hereby acknowledge that I have read and understand Chapter 8, MSC INFOSEC and COMSEC CMS Policy and Procedures, contained in reference (a).

2. I assume full responsibility for the proper handling, storage, inventorying, accounting and disposition of COMSEC material held in my custody and/or used by me.

3. If at anytime I am in doubt as to the proper handling of COMSEC material that I am responsible for, I will immediately contact the EKMS Manager by E-mail at _____or by phone at (757) 417-4395/4706 (DSN 537) and request advice.

4. Before any extended departure from the command (i.e., permanent transfer or leave/TAD/ TDY in excess of 30 days), I will report to the EKMS Manager and be relieved of responsibility for all COMSEC material I have signed for.

SIGNATURE_____

DATE_____

Copy to
AOR Primary Tier 3 EKMS Manager
Ship's File

Form B:

CMS RESPONSIBILITY ACKNOWLEDGMENT FORM- (STU/STE Only)

FROM: _____
(RANK/RATE, Full Name, SSN, and Command of CMS User)

TO: MSC CMS HOLDER / EKMS Manager Account (local)

SUBJ: CMS RESPONSIBILITY ACKNOWLEDGMENT

REF: (a) COMSCINST 2000.2

ENCL: (1) CMS Responsibilities and Duties of STU/STE Holders

1. I hereby acknowledge that I have read and understand enclosure (1), CMS Responsibilities and Duties of STU/STE Holders.

2. I assume full responsibility for the proper handling, storage, inventorying, accounting and disposition of COMSEC material held in my custody and/or used by me.

3. If at anytime I am in doubt as to the proper handling of COMSEC material that I am responsible for, I will immediately contact the EKMS Manager by E-mail or by phone and request advice.

4. Before any extended departure from the command (i.e., permanent transfer or leave/TAD/ TDY in excess of 30 days), I will report to the EKMS Manager and be relieved of responsibility for all COMSEC material I have signed for.

SIGNATURE_____

DATE_____

Copy to:
AOR Primary Tier 3 EKMS Manager
Ship's File

CMS RESPONSIBILITIES AND DUTIES: USER PERSONNEL

CMS User are responsible for the proper security, control, accountability and disposition of all COMSEC material they handle whether or not they signed for the material.

All CMS Users must complete a CMS Responsibility Acknowledgment Form.

CMS Users are responsible for the following specific duties:

- Comply with the applicable security, control and accountability procedures of all written instructions provided by EKMS Manager or higher authority.
- Ensure the proper inventory and destruction of COMSEC material received on local custody.
- Complete, maintain and forward required accounting records and reports to the EKMS Manager.
- Ensure proper storage and adequate physical security is maintained for COMSEC material.
- Ensure adherence to TPI requirements.
- Conduct training to ensure that all personnel using STU/STE equipment are familiar with and adhere to the procedures set forth below.

STU/STE Background

The STU III and its replacement STE are in use throughout MSC for secure voice and messaging services. The STU III equipment, as long as it is un-keyed, can be handled as a valuable component but must be accounted for as CCI. The Key Storage Device or KSD-64 is the physical device that can be used as a Fill Device (FD) and also as a Crypto Ignition Key (CIK). It is a small device shaped like a physical key and contains passive memory.

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 KOV-14 cryptographic card that provides all the security services. The STE is a high dollar-value sensitive, pilferable item; therefore, standard Department of Defense and Navy logistics, property accounting and security controls must be strictly adhered to.

Classification and Handling

For the STU-III, three conditions affect its security classification:

- With no keying material loaded, the terminal is unclassified.
- With keying material installed, but not its associated CIK, the terminal is unclassified.
- With keying material installed and associated CIK inserted, the terminal is classified to the level of the key loaded.

Keying Material

Type 1 Seed Key is used by MSC. It is designated UNCLAS CRYPTO and may be shipped and handled as such. However, Seed Key must be stored at the level to which it can be converted. This level is identified by the classification markings on the attached tag. Seed Key allows secure calls between terminals only after a conversion call to the EKMS CF has taken place after initial loading. The conversion call actual places operational key into terminal utilizing the information supplied on the Seed Key and data provided to the terminal from the EKMS CF during the conversion call.

Once keying material has been successfully loaded into a terminal and properly reported as destroyed (by SF 153 or by a successful conversion call), the keying material is no longer accountable to EKMS CF.

For the STE

The terminal security conditions are similar to the STU III; however, the device utilizes a Fortezza Plus card rather than a CIK.

The KOV-14 card is assigned Accounting Legend Code 1 (ALC-1). This means that the KOV-14 card must be accounted for within the COMSEC Material Control Systems (CMCS) by its unique serial number, not the keying material identification number on the tags, until the card is physically destroyed.

A KOV-14 card may be a fill, user, carry, TPA or un-keyed (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.

A Fill card is a keyed KOV-14 card that has not been associated with an STE. A Fill card may be programmed with Seed, Test or Operational keying material and accountable to the COMSEC Account's Central Office of Record (COR). A COMSEC Holder or TPA 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 an STE.

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.

Inventory

To prevent the lost of accountability, COMSEC material will be inventoried daily and must be documented.

Storage

Storage space for CMS material shall provide maximum protection against unauthorized access, material damage, deterioration and destruction. Unless COMSEC material is under the direct control of authorized persons, keep the container and spaces locked.

Store COMSEC material separately from other classified material, and only in containers approved for storage. Loaded and unloaded COMSEC FDs will also be stored in a TPI container. The storage container will be free of external markings, which indicate the classification and status.

Storage containers for COMSEC material require the following forms:

- Standard Form 700. Classified container information form which must be placed on the inside of each COMSEC storage container.
- Standard Form 702 S.
- OPNAV Form 5510/21.

Receipt

Inspect the inner wrapper for signs of tampering. Signs of tampering immediately contact EKMS Manager.

Open the shipment.

Inventory the contents against the enclosed SF-153, if information is correct.

Authorized user must sign and date enclosed SF-153, send back to EKMS Manager within 96 hours of receipt.

Apply status information (less equipment).

Add COMSEC to running inventory.

Properly store the material.

Transfer

An SF-153 will be used by LEs for any material returned to main account.

Ensure the following information is applied:

- Transfer: block 1
- Issued by: block 2
- Date of report: block 3
- Issued to: block 7
- Short title: block 9
- Quantity: block 10
- Accounting number: block 11
- ALC code: block 12

Routine Destruction

Effective and superseded keying material is extremely sensitive, and if compromised, potentially exposes all information encrypted by the material. COMSEC material authorized for destruction must be destroyed by two properly cleared and authorized people (one person must be E-5/GS-5 or above). Destruction documentation (SF-153) will be sent to the EKMS Manager.

8.9.3 Over-the-Air- Receipt/Transfer (OTAR/OTAT) Local Receipt, Delivery, Relay Record

Ref. 8.5.2.2

CONFIDENTIAL (When filled in)

RELAYING/RELOADING STATION OTAR/OTAT LOG FOR THE MONTH OF _____

1. KEY ID SHORT TITLE	2. CA	3. CLASS	4. CIRCUIT KEY INTENDED FOR	5. EFF PD	6. DATE/TIME RECEIPT (R) TRANSMISSION (T)	7. CIRCUIT I.D. TRANSMITTED OVER RECEIVED	8. STORAGE POSITION AND FILL DEVICE SERIAL NO	9. ZEROIZED DATE/TIME	10. INITIALS

PAGE_____OF_____

CONFIDENTIAL (When filled in)

8.9.4 Data Transfer Device (DTD) OTAT Log

Ref. 8.5.3.2

CONFIDENTIAL (When filled in)

RECEIVING STATION OTAT LOG FOR THE MONTH OF _____

KEY SHORT TITLE	ED	SEGMENT NUMBER	CLAS	EFFECTIVE PERIOD	DELETE ON DATE	DATE DELETED	OPR/WITNESS 2 INITIALS	

PAGE_____OF_____

CONFIDENTIAL (When filled in)

8.9.5 SF 153 COMSEC Material Report Form and Directions for Use

Refer to Sections 8.4.4.5 and 8.5.4.5.

Directions for Using SF 153 (COMSEC Material Accounting Report)

1. **SF 153 (COMSEC Material Accounting Report)**. There are currently two versions of the preprinted SF 153 authorized for use; one reflects a revision date of 9-79 and the other 9-88. Both versions contain identical data blocks of information but are assigned different numbers. A computer-generated SF-153 (10-95) is also available and is provided below together with a sample Transfer Report.

2. **Verifying for 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, transactions numbers, signatures or the report contains errors in the short title(s) or accounting data) forwarded to DCMS cannot be processed until all errors or omissions are corrected.

c. Changes or corrections to an SF 153 must be reported to DCMS//30// via message or facsimile.

3. **Assigning Transaction Numbers (TNs)**. CMS TNs maintain the continuity of COR reportable transactions within each CMS account and provide a means of verifying individual account records.

4. **Line Entries on SF 153 Accounting Reports**

a. Material must be listed one item per line on all SF 153 Accounting Reports.

b. If multiple copies of an edition of an AL 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 AB 888 344-346").

c. If accounting numbers are not in consecutive sequence (i.e., sequential number series is broken), a separate line entry is required for each.

d. For AL 2 and AL 4 material (accountable by quantity), list multiple copies of the same short title and edition as a single consolidated line entry.

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 line 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.

5. **Signature Requirements**

a. Inventory, Destruction, Possession Reports Generated/Submitted as the Result of a Found Material COMSEC Incident, and all Relief from Accountability Reports

(1) Require the signature of two Holders or a Holder and a properly cleared witness, and the Commanding Officer/OIC/SCMSRO, as appropriate.

(2) In the absence of the Commanding Officer, the Executive Officer is authorized to sign accounting reports as “Acting” Commanding Officer.

(3) Accounting reports which are signed by the SCMSRO must be annotated to reflect "Staff CMS Responsibility Officer” vice by direction or acting.

b. Reports Listing SAS/TPC Material

(1) SF 153 Transfer/Receipt and Destruction reports which 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 CMS Holder for use in reporting the transfer or receipt of SAS/TPC material to DCMS. (NOTE: CJCSI 3260.1 contains basic accounting and control guidance for SAS/TPC material.)

c. Other Reports. SF 153s used to document the receipt of Top Secret CRYPTO require two signatures: the CMS Holder (or alternate acting on his/her behalf) and a witness. All other SF 153s require only one signature, the CMS Holder or Alternate Holder acting in his/her behalf.

d. All accounting reports submitted to DCMS must be signed and be original copies.

e. Signatures generated by means of a signature stamp or other signature device 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.

6. **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., Possession).

b. **Block 2 – From**. Enter your account command title, complete mailing address and CMS account number.

NOTE: If a "Local" SF 153 Accounting Report (e.g., local destruction, local inventory) is being prepared, the CMS account number may be omitted.

c. **Block 3 - Date of Report**. Enter the date as year, month and day (e.g., 930815). Reports generated by ANCRS will display the last digit of the calendar year and the Julian date following the year, month, day entry. Complete Block 3 as indicated below for the following reports:

(1) Transfer reports. Completed by the originator of the transfer and must reflect the date that the report was actually prepared.

(2) Receipt reports. Completed by the recipient of an SF 153 Transfer Report and must reflect the date the SF 153 is being signed.

(3) Destruction reports. 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 local holders or Users), date of report preparation is acceptable.

(4) Possession, Relief from Accountability, Conversion and Inventory Reports. Completed by the originator and must reflect the date the SF 153 is being signed.

d. **Block 4 - Outgoing TN**. This block may be left blank or assigned a local TN.

e. **Block 5 - Date of Transaction**. For recipients of Transfer 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**. This block may be left blank or assigned a local TN.

g. **Block 7 - To**

(1) For SF 153 Transfers. Enter the command identification, complete mailing address and the CMS 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 Local Holder/User.

(3) For SF 153 Possessions, 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.

(5) For SF 153 Destructions. If preparing the report for submission to DCMS, insert "CMS DESTRUCTION" and insert the 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.

(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., CSMR, originator and date-time-group of message).

(b) Transfer Reports. Cite transfer authorization.

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 – ALC**. 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**. For all reports, less transfers, enter "CMS Holder."

(1) Blocks 15a & 15b. Signature of Holder 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 & 15d. Enter the name of the Holder and branch of service, if applicable.

p. **Block 16 – Witness**. Place an "x" in the box marked "Witness" when receipting for Top Secret Crypto or SAS/TPC material and for Possession (generated/submitted as the result of a Found Material COMSEC incident), Destruction, Inventory, Conversion and all Relief from Accountability Reports.

q. **Block 17 - Commanding Officer Signature data**. The signature of the Commanding Officer, SCMSRO or OIC, as applicable, is required only on Destruction, Inventory, Possession (generated/submitted as the result of a Found Material COMSEC incident) and all Relief from Accountability Reports.

r. **Block 17 - Page number information**. Enter the appropriate page number information (e.g., Page 1 of 1).

COMSEC MATERIAL REPORT - This form is FOR OFFICIAL USE ONLY unless otherwise stamped.

1. [ ] TRANSFER [ ] INVENTORY [ ] DESTRUCTION [ ] HAND RECEIPT [ ] OTHER							
2. FROM		ACCT. NO.		4. DATE OF REPOR		5. OUTGOING NBR	
				6. DATE OF TRANS.		7. INCOMING NBR	
3. TO		ACCT. NO.		ACCOUNTING LEGEND CODE 1. ACCOUNTABLE BY SERIAL NUMBER 2. ACCOUNTABLE BY QUANTITY 4. INITIAL RECEIPT CONTROL			
	9. SHORT TITLE/DESIGNATOR/EDITION	10. QUANTIY	11. ACCOUNTING NUMBERS BEGINNING NBR	ENDING NBR	12. ALC	13. REMARKS	
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
14. THE MATERIAL HEREON HAS BEEN [ ] RECEIVED [ ] INVENTORIED [ ] OTHER							
15. AUTORIZED RECIPIENT			16.[ ] RECIEVED [ ] INVENTORIED [ ] OTHER				
a. SIGNATURE		b. GRADE	a. SIGNATURE			b. GRADE	
a. TYPED OR STAMPED NAME		d. SERVICE	a. TYPE OR STAMPED NAME			d. SERVICE	
17. FOR DEPARTMENT OR AGENCY USE							

PAGE 1 OF 1 PAGES

This form is FOR OFFICIAL USE ONLY unless otherwise stamped **Computer Generated SF 153 (10-95)**

COMSEC MATERIAL REPORT - This form is FOR OFFICIAL USE ONLY unless otherwise stamped.

1. [X] TRANSFER [ ] INVENTORY [ ] DESTRUCTION [ ] HAND RECEIPT [ ] OTHER

2. FROM MSC SHIP	ACCT. NO. 370006-XXX	4. DATE OF REPOR YYYYMMDD	5. OUTGOING NBR YY-##
		6. DATE OF TRANS.	7. INCOMING NBR
3. TO EKMS Manager	ACCT. NO. 370006-XXX	ACCOUNTING LEGEND CODE 1. ACCOUNTABLE BY SERIAL NUMBER 2. ACCOUNTABLE BY QUANTITY 4. INITIAL RECEIPT CONTROL	

	9. SHORT TITLE/DESIGNATOR/EDITION	10. QUANTIY	11. ACCOUNTING NUMBERS BEGINNING NBR	ENDING NBR	12. ALC	13. REMARKS
1	STU-N10	1	000001	000001	1	
2						
3	NOTE: Transfer IAW COMSC EKMS MGR					
4	Virginia Beach					
5	251306ZMAR02					
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						

14. THE MATERIAL HEREON HAS BEEN [ ] RECEIVED [ ] INVENTORIED [ ] OTHER

15. AUTORIZED RECIPIENT		16.[ ] RECIEVED [ ] INVENTORIED [ ] OTHER	
a. SIGNATURE EKMS Holder	b. GRADE	a. SIGNATURE Witness	b. GRADE
a. TYPED OR STAMPED NAME	d. SERVICE	a. TYPE OR STAMPED NAME	d. SERVICE

17. FOR DEPARTMENT OR AGENCY USE

PAGE 1 OF 1 PAGES

This form is FOR OFFICIAL USE ONLY unless otherwise stamped **Computer Generated SF 153 (10-95)**

8.9.6 CMS-25/One-Time Keying Material Destruction Report

CONFIDENTIAL (When filled in)

CMS-25/ONE-TIME KEYING MATERIAL DESTRUCTION REPORT

Retain this form with material locally until complete destruction of material is documented on SF153. These individual one-time keying material cards or segments were destroyed on the dates and by the two individuals indicated below:

CARD #	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				

Short title:_____Reg#/Accounting#:_____ AL Code:_____

Grade/Signature_____ Grade/Signature_____

Declassify on: _____

CONFIDENTIAL (When filled in)