



UNITED STATES MARINE CORPS

I MARINE EXPEDITIONARY FORCE
U. S. MARINE CORPS FORCES, PACIFIC
BOX 555300
CAMP PENDLETON, CA 92055-5300

IN REPLY REFER TO
I MEFO 2281.1
G-6 MCMO

AUG 20 2009

I MARINE EXPEDITIONARY FORCE ORDER 2281.1

From: Commanding General, I Marine Expeditionary Force
To: Distribution list

Subj: COMMUNICATION SECURITY STANDARD OPERATING PROCEDURES
(COMSEC SOP)

Ref: (a) EKMS 1 (Series)
(b) EKMS 3 (Series)
(c) MCO P4400.15E
(d) MFPO 2280.E
(e) SECNAVINST 5510.36
(f) OPNAVINST C5510.93F
(g) EKMS 5 (Series)
(h) MCO P5510.14
(i) MCO P5530.14

Encl: (1) COMSEC Definitions
(2) Official Correspondence
(3) OTAR/OTAT Logs
(4) Check List
(5) Procedures For routine Modification of COMSEC Allowance

1. Situation. To set forth the Communication Security (COMSEC) SOP and objectives of Commanding General, I Marine Expeditionary Force (MEF) and to assign the responsibilities necessary to accomplish communications security.

2. Mission. All I MEF commands with Electronic Key Management System (EKMS) accounts and those commands that provide oversight shall review and comply with this Order. This Order is based on references (a) through (g) and does not replace their guidance and procedures. Detailed instructions for accountability, destruction, distribution, filling, generation, management, ordering, storage and usage of keying material (keymat), and reporting are specifically outlined in references (a) and (b).

3. Execution

a. Commanders Intent and Concept of Operations

(1) Commanders Intent. To provide guidance on the management of the Electronic Key Management System (EKMS) inspection program, training, and proper management of EKMS accounts in order to mitigate COMSEC insecurities.

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

COMSEC is designed to deny unauthorized persons information of value which might be derived from the possession and study of communications. Use of any communications system, secure or un-secure, must include COMSEC measures so that enemy exploitation is difficult and time-consuming.

(2) Concept of operations. Strict adherence to all established national and Department of the Navy policies and procedures are mandatory. In order to ensure the effective and efficient use of COMSEC during every exercise and operation, and to ensure protection of telecommunications, cryptographic equipment, keying material, and national security, leaders and managers shall follow these leadership concepts:

(a). Momentum (i.e., how well EKMS designees respond to direction). Reinforce every positive behavior until all Managers and Local Elements reach high and steady rates of performance. Develop a system for discovering Marines who are giving discretionary effort (i.e., the difference between how well designees actually perform and how well they are capable of performing) to assure compliance with policy and procedures.

(b). Commitment (i.e., are the EKMS designees focused on following established guidelines and procedures). Publicly recognize Marines who exemplify COMSEC policies and EKMS procedures through their actions or decisions. Consider lack of focus or non-compliance as a reflection of too little reinforcement received for behavior that is not within established guidelines or procedures.

(c). Teamwork (i.e., are the EKMS designees working together). Recognize high-performing Marines and publicize their accomplishments.

(d). Reciprocity (i.e., are the EKMS designees collectively working with leadership). Make hard work rewarding by expressing personal interest and showing enthusiasm for the work Marines do to stay within compliance. Solicit feedback from Immediate Superior in the Chain of Command (ISIC)/Inspectors and Managers about any actions that should be started, stopped, or continued.

b. Tasks

(1) Commanding Officer (CO), Officer-in-Charge (OIC). The Commanding Officer is responsible for properly administering their command's Communication Security Material Systems (CMS)/EKMS account and ensuring compliance with references (a) through (f). Annex D of reference (a), is written specifically for Commanding Officers, and contains a CMS/EKMS account assurance checklist for use in assessing their command's compliance with the provisions of references (a) through (f). COs and OICs must:

(a). Appoint qualified individuals in writing as EKMS Manager, Alternates, Digital Transfer Device (DTD) Supervisory Crypto Ignition Key (CIK) users, Site Security Officer (SSO) and Account Clerk as outlined in reference (a).

(b). Establish a list of personnel authorized access.

(c). Ensure COMSEC incident reports (i.e., Initial or Amplifying) are promptly and accurately submitted to appropriate officials, including I MEF G6. Submit COMSEC incident reports as outlined in reference (a).

This report is exempt from reports control under SECNAV M-5214.1, Part IV, paragraph 7.d.

(2) Staff CMS Responsibility Officer (SCMSRO). A Flag or General Officer in command status, or any officer occupying the billet of a Flag or general Officer with command status, may either assume personal responsibility for routine CMS matters or may designate the responsibility to a Senior Staff Officer [O-4 (or selectee)/GS-12 and above]. Officers not meeting the above requirement may not designate a SCMSRO.

(3) Immediate Superior in Command (ISIC). Responsible for the administrative oversight of all COMSEC matters for their subordinate commands by:

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

(b). Determining COMSEC material allowance requirements and, when required, obtaining Controlling Authority (CONAUTH) authorization per reference (a).

(c). Ensuring that physical security inspections are conducted annually.

(d). Conducting EKMS account inspections and forwarding copies of reports of inspection findings to Headquarters Marine Corp C4 IA via the chain of command.

(e). Reviewing and/or retaining COMSEC records pending receipt of Naval Communication Material Systems notice of reconciliation upon account disestablishment.

(4) CMS/EKMS Managers. A CMS/EKMS manager is an individual designated in writing by the CO to manage COMSEC material issued to a CMS/EKMS account. The EKMS manager may or may not hold the Military Occupational Specialty (MOS) 0681. The CMS/EKMS Manager is the CO's primary advisor on matters concerning the security and handling of COMSEC material and the associated records and reports.

(5) Alternate Manager(s). The individual(s) designated in writing by the CO is responsible for assisting the CMS/EKMS manager in the performance of their duties and assuming the duties of the CMS/EKMS manager in their absence. Alternate custodians share equally with the CMS Custodian the responsibility for the proper management and administration of a CMS/EKMS account.

(6) CMS/EKMS Clerk. An individual designated in writing by the CO who assists the CMS/EKMS Manager and Alternate(s) with routine administrative account matters. Appointment of a CMS Clerk is not mandatory, but is at the discretion of the CO. CMS/EKMS Clerks will not be granted access to COMSEC material, i.e., they can not possess combinations to secure spaces, administer or operate the Local Management Device/Key Processor (LMD/KP), issue, courier or possess keying material in "black" form.

(7) CMS/EKMS Users. An individual designated in writing by the CO who, regardless of whether or not they personally signed for COMSEC material, requires COMSEC material to accomplish an assigned duty and has obtained the material from a custodian or another user on local custody. CMS Users must

comply with the procedures for the handling and accountability of COMSEC material placed in their charge.

(8) CMS Witness. Any properly cleared U.S. Government employee (military or civilian) who may be called upon to assist a custodian or user in performing routine administrative tasks related to the handling of COMSEC material. A witness must be authorized, in writing, access to keying material.

(9) CMS/EKMS Account. A CMS/EKMS account is an administrative entity, identified by a six-digit account number, in which custody and control of COMSEC material are maintained.

(10) Local Element (LE). LE accounts are separate units or commands that require COMSEC material and function essentially as sub-accounts of a numbered CMS account. LE accounts are managed in much the same way as a CMS account except they are not assigned a CMS account number and normally receive their COMSEC material from a parent CMS account.

(11) Digital Transfer Device (DTD) Supervisory User. Unrestricted access to Supervisory Crypto Ignition Keys must be limited to those individuals who are designated in writing by the CO/SCMSRO to perform all of the privileges allowed by the Supervisory CIK.

(12) Site Security Officer (SSO). The AN/PYQ-10 (Simple Key Loader) and/or KIK-20 audit trail must be reviewed monthly, and the reviews documented by the SSO. Audit reviews must be documented in a review log and retained for a minimum of two years. If the SSO is different from the EKMS Manager he/she must be designated in writing by the CO/SCMSRO as an authorized SSO/Supervisory User.

(13) EKMS Manager and Alternate Manager Designation Requirements. For Marine Corps EKMS accounts, the designated manager must be an E-6 or above. Alternate managers must hold a military grade of at least E-6. Civil servants must meet equivalent grade requirements. The CO/OIC will not designate personnel currently serving as EKMS Manager and Primary Alternate EKMS manager to serve simultaneously as managers of more than one EKMS account.

4. Administration and Logistics

a. Required Files and Accounting

(1) EKMS. The EKMS provides the capability for automated generation, accounting, distribution, destruction, and management of electronic key, as well as management of physical key and non-key COMSEC-related items. The Local Management Device (a computer suite)/Key Processor (KOK-22A) (LMD/KP) is an important part of the EKMS. The LMD/KP will provide users the capability to perform and access EKMS services located at the Central Facility in Finksburg, MD. The LMD utilizes the Santa Cruz Operation Universal Network Information Exchange (SCO UNIX) based software program local COMSEC Management System. As EKMS becomes fully operational, key management will begin to transition from manually intensive, service-unique activities, to automated, common and highly interoperable ones. Reference (a) is effective 27 March 2007 for CMS accounts operating with EKMS components. The DON is the Executive Agent for the EKMS system, when fully implemented the system will encompass the entire Department of Defense. When fully implemented the system will be:

(a). Common Tier 0. Central Facility, National Security Agency and Finksburg key facilities which provides centralized key management services for all forms of key.

(b). Common Tier 1. Central Office of Record (COR), serves as the intermediate key generation and distribution center, Privilege Certificate Manager, and Registration Authority for EKMS Tier 2 accounts. Located at Ft. Huachuca, AZ and Kelly AFB TX.

(c). Common Tier 2. Numbered CMS/EKMS accounts that use the Local Management Device/Key Processor (LMD/KP).

(d). Common Tier 3. The lowest layer of the EKMS architecture that includes the Digital Transfer Device (DTD) and all other means used to transfer key to cryptographic equipment.

(2) Limitations. This order cannot address every conceivable situation that might arise in the daily handling of COMSEC material. When unusual situations confront a Manager or Local Element, the basic tenets applicable to the protection of classified information should be implemented until definitive guidance is provided by NCMS or other authoritative source (e.g., material's controlling authority, Combatant Commander, and ISIC).

(3) General Control. COMSEC material must be handled and safeguarded based on its assigned classification and Accounting Legend (AL) Code. COMSEC material is centrally accountable to the NCMS and the command's EKMS account. Control of COMSEC material is accounted for through a continuous chain of custody receipts using transfer reports (SF-153's and CMS-17 cards), local custody documents, accounting records, periodic inventory reports, and destruction records. Immediately report any COMSEC material incident to the controlling authority/evaluating authorities for the material.

(4) Accounting Legend Codes (ALC). AL codes determine how COMSEC material is accounted for within the CMS system. There are five AL codes that are used to identify minimum accounting controls required for the COMSEC material. For more information see reference A.

(5) CRYPTO Markings. The marking "CRYPTO" identifies all COMSEC keying material which is used to protect or authenticate classified or sensitive unclassified government or government derived information, the loss of which could adversely affect national security. All classified paper keying material marked "TS CRYPTO" and above requires Two Person Integrity (TPI).

(6) Controlled Cryptographic Items (CCI). CCI is the designator that identifies secure telecommunications or information handling equipment, or an associated cryptographic component. CCI equipment must be stored in a manner that affords protection against pilferage, theft, sabotage or tampering, and ensures that access and accounting integrity is maintained. This equipment also requires dual accountability and must be accounted for by the units G-4, S-4 or Supply personnel as appropriate. The majority of CCI items have embedded cryptographic chips in them, for example; SINCGARS RADIOS (RT-1523). Along with the SL-3 items, equipment must be accounted for on the units Table of Equipment and local Consolidated Memorandum Report.

(7) Status of COMSEC Material. Status of COMSEC material is assigned at the direction of the Controlling Authority or originator of the material. COMSEC keying material will, at all times, be in one of the following three conditions:

(a). Reserve. Held for future use.

(b). Effective. In use to support an operational requirement.

(c). Superseded. No longer authorized for use; must be immediately destroyed (see reference (a)). Superseded material is normally the most inherently dangerous phase in the life of COMSEC material. Particular caution must be used to ensure the proper accounting, safeguarding, and destruction of this material. The late destruction of COMSEC material is a Practice Dangerous to Security (PDS). Before filling the PDS report ensure it's reviewed and signed by the CO/SCMSRO.

(8) Reserve on Board (ROB). ROB is a quantity of keying material, not yet effective, held in reserve by an account for use at a later date. All accounts are required to maintain the current month plus three months ROB at all times.

b. Safeguarding COMSEC Material

(1) Responsibility. Each person involved in the use of COMSEC material is personally responsible for safeguarding and properly using the material for which they are responsible for and promptly reporting any COMSEC material incident to proper authorities.

(2) Access and Release Requirements for COMSEC Material. Access to classified COMSEC material requires a security clearance equal to or higher than the classification of the COMSEC material involved. Access to unclassified COMSEC material does not require a security clearance. Revocation of a security clearance revokes access to classified COMSEC material.

(a). The CO or SCMSRO must authorize all personnel having access to COMSEC keying material in writing. An individual letter or access list may be used for this authorization, and the original retained by the EKMS Manager.

(b). U. S. citizens who are military personnel may be granted access to COMSEC material if they are properly cleared and their duties require access. Resident aliens, who are military personnel, may be granted access to COMSEC material classified no higher than CONFIDENTIAL.

(3) Access to COMSEC Equipment (LESS CCI). Access to keyed and unkeyed COMSEC equipment may be granted to those whose official duties require access and who possess a security clearance equal to or higher than the classification of the equipment. In addition, access to keyed COMSEC equipment requires a clearance equal to or higher than the classification of the equipment or keying material. An un-cleared individual may have access to keyed CCI equipment in the performance of their duties. The access is called "Incidental Operator" access and is granted for vehicle crewman (i.e., Tank Crewmen, LAV Crewmen can have access to SINCGARS Radios) and others that require access to the COMSEC equipment, but not the keying material, in the performance of their duties.

(4) Two Person Integrity (TPI) Requirements. TPI is a system of handling and storing designed to prevent single person access to Top Secret COMSEC material marked "CRYPTO". TPI handling requires at least two properly cleared individuals to be in constant view of each other while the keying material is not locked up in a TPI safe. TPI storage requires using two

approved combination locks (each with a different combination) or the Mas-Hamilton X07, 08 or 09 with no one person authorized access to both combinations.

(5) Incidental Operators. With the fielding of SINCGARS and other radios with embedded crypto, the Marine Corps has been confronted with the need to allow incidental operators without appropriate security clearances to have access to keyed crypto equipment. National policy governing access to classified cryptosystems has been relaxed by the 30 May 1997 National Security Telecommunications Information Systems Security Issuance (NSTISSI). This policy states:

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

(b). In a tactical environment, supervision of an appropriately cleared person may not always be possible (e.g. an un-cleared driver may need to operate keyed radio equipment as part of a convoy; a contact team driver and mechanic may find it necessary to operate keyed radio equipment to effect contact team mission; an un-cleared member of an infantry company Head Quarters may need to operate the company or Battalion Tactical radio equipment, etc.). Therefore, the following additional guidance is provided for Marines in a tactical environment or exercise.

(1). COs may authorize operation of keyed voice radio equipment by individuals who do not possess the appropriate security clearance provided the following guidance is adhered to:

a. The individual's official duties must require access as an operator of the equipment (e.g., Tank/AAV Crewmember, Forward Observer, etc).

b. The net on which the radio is operated is a tactical or security radio net.

c. The individual is indoctrinated in the handling and safeguarding of COMSEC material by the EKMS Manager or ALT Manager.

d. The individual signs an Incidental Users Form. See enclosure (2) for an example.

(2). Indoctrination and signing of the form must be completed prior to an individual gaining access to keyed radio equipment except during emergency combat situations.

(3). Material must be issued on a local custody issue form. Material should be issued to an appropriately cleared person. Under no circumstance will un-cleared individuals be authorized to handle classified keying material or fill devices with classified key fill.

(6) Access to and Protection of Safe Combinations. Each lock must have a combination composed of randomly selected numbers based on manufacturer's instructions. The combinations will not duplicate another

lock or safe within the command and will not be composed of successive numbers, systematic sequence, or predictable sequences.

(a). Combinations will be changed when any person having knowledge of the combination no longer requires access, or when the possibility exists that the combination has been subjected to compromise, or at a minimum, every two years.

(b). Only properly cleared and authorized personnel will have knowledge of and access to combinations protecting COMSEC material. Lock combinations shall be classified and safeguarded at the same as the highest classifications of the material being protected.

(c). To provide emergency access to combination envelopes, the lock combinations must be maintained in a security container other than the container where the CMS material is stored. A monthly visual check is required to ensure no tampering or compromise of the envelope.

(d). The combination envelope (SF-700) will be sealed, wrapped and packaged per reference (a), chapter 5.

(7) Storage Requirements. COMSEC material will be stored in General Service Administration approved containers and spaces approved for CMS material per (a) through (f). Store COMSEC material separately from other classified material.

(a). The COMSEC Vault must have a Physical Security Survey (PSS). Aboard Marine Corps installations, physical security surveys will be conducted on an annual basis by school-trained military police personnel possessing MOS 5814 (Physical Security/Crime Prevention Specialist) and a Secret Clearance.

(b). A SF - 700 form must be placed on the inside of each COMSEC storage container to include appropriate Privacy Act Information.

(c). A SF - 702 form must be maintained for each COMSEC storage container.

(d). Office of Personnel (OP) form 89 must be maintained for each COMSEC storage container. This is a permanent record for the container.

(e). A SF - 701 form must be maintained for each vault or strong room.

(f). The Mas-Hamilton electro-mechanical combination lock, meeting Federal Specifications FF-L-2740, is the preferred type of lock to be used.

(8) Courier Responsibilities. Couriers shall be designated in writing and have the same or higher clearance than the material being carried. DD Form 2501 may also be used. Contact your unit Security Manager for rules, responsibilities, and briefing on courier duties.

(9) Physical Security Survey (PSS). Approval to hold classified COMSEC material must be approved by the ISIC to hold classified COMSEC material prior to its use. This approval should be based upon a physical security inspection that determines whether or not the facility meets the physical safeguarding standards of reference (a). After the initial approval, periodic re-inspections will be conducted based on threat, physical

modifications, and sensitivity of programs and past security performance. The facility must be re-inspected and approved when there is evidence of penetration or tampering, after alterations that significantly change the physical characteristics of the facility, when the facility is relocated or when it is reoccupied after being temporarily abandoned.

(a). Reference (i) states "a physical security survey is a systematic evaluation of the overall security of a given facility or activity and should not be regarded as an inspection or investigation. Surveys identify deficiencies and corrective measures to the commander". Also that "Aboard Marine Corps installations, physical security surveys will be conducted on an annual basis by school-trained military police personnel possessing MOS 5814 (Physical Security/Crime Prevention Specialist) and a Secret clearance".

(b). The ISIC will provide all EKMS accounts within its responsible area with written authorization to hold COMSEC material up to the Highest Classification Indicator (HCI) of the EKMS account. ISIC's will authorize a facility to hold COMSEC material at a minimum of every 12 months.

(c). The Unit Security Manager authorizes the facility to be "Open Storage" based on the PSS, per reference (e).

(10) CO's Spot Checks. The CO will conduct Spot Checks provided in Annex D of the EKMS-1A. Unannounced spot checks will be conducted on a monthly basis. The CO can delegate eight of the spot checks to the Executive Officer and Communications Officer, but must perform at least four Spot Checks personally.

(11) Inspections. Per references (a) and (b) only certified EKMS Inspectors can inspect an EKMS account. All DON EKMS accounts must receive an unannounced EKMS inspection once every twenty-four months. In order to increase the oversight, awareness by Marines and Sailors, and assess the readiness of I MEF EKMS accounts, each ISIC is required to inspect all EKMS accounts within their area of responsibility (Division, Marine Air Wing, and Marine Logistics Group) on an annual basis. ISICs are to provide the information stated in reference (b) to this office semi-annually unless otherwise directed. Reports are due the months of July and January.

(12) COMSEC Incident. All COMSEC Incidents will be reported per Chapter nine of reference (a). All incidents will have a Preliminary Investigation done at a minimum. The results will be reported in writing to the unit's ISIC.

(13) Destruction. The EKMS Manager and Alternates are responsible for the complete and prompt destruction of all CMS material in their custody when it is authorized for destruction. This destruction will be conducted per Article 250 and 255 of reference (a). Emergency supersession is an entirely different matter you must check the SIPRNET daily for emergency supersession messages. In any event, all routine destruction of COMSEC material will comply with the applicable provisions listed in references (a) and the Controlling Authorities status message.

(a). Destruction of an entire short title that has not been issued for use must be destroyed as soon as possible or within five working days of its supersession as a unit (whole edition). This includes unopened daily keying material, publications, which are not superseded on a daily basis as well as electronic key in the Key Processor (KOK 22A).

(b). Equipment must be destroyed when specifically directed to by NCMS WASHINGTON DC. NCMS and Controlling Authority (CA) directives require the destruction of daily keying material (segmented) within 12 hours after supersession. In order to facilitate compliance with this requirement, users are authorized to destroy keying material held in their custody, and provide the EKMS Manager with the destruction report, SF-153 or CMS 25 form. The SF-153 or CMS 25 forms with all the required data are the only forms to be used to record the destruction of primary keying material. This includes daily, weekly and monthly destructions.

(c). In all cases, it is mandatory that two properly cleared and indoctrinated persons jointly sight each individual piece of CMS material, verify it has been superseded, and witness its destruction. After the destruction, both witnesses must affix their signatures on the SF-153 or CMS 25 form. In order to avoid unauthorized destruction, it is essential that each item being destroyed be visually verified immediately prior to destruction.

(14) Verifying Destruction. The individual responsible for destruction and the witness must verify the superseded status of and the accounting data of the material being destroyed. Both persons are responsible for the timely and proper destruction of the material and for the accuracy of the destruction records. To verify the material being destroyed against the destruction record, the individual responsible for the destruction should read the short titles and accounting data of the material being destroyed to the witness who verifies the accuracy and completeness of the entries on the destruction report. The witness should then read the short titles and accounting data of the material being destroyed to the individual responsible for the destruction who then verifies the accuracy and completeness of the entries on the destruction report. The individual responsible for the destruction and the witness must follow the procedures specified in EKMS 704C, LMD/KP Operators Manual, for the destruction of electronic key that is still on the system. All copies of issued or reissued keying material must be destroyed prior to completing system destruction procedures.

(15) Witnessing Destruction. The two people conducting the destruction of COMSEC material may not complete corresponding destruction records until the material is actually destroyed. Therefore, the two people conducting the destruction must personally witness the complete destruction of the material. The CO is ultimately responsible for everything that happens or does not happen within the account, therefore, the Commanding Officer or Staff CMS Responsibility Officer must also sign the SF - 153 verifying the material has been destroyed.

(16) Monitoring and Inspection of Destruction Devices. Monitor the entire destruction process and inspect the destruction device and the surrounding area afterward to ensure destruction is complete and no material is inadvertently missed during the destruction process. Inspect the residue to ensure destruction is complete, and no residue or readable bits of material remain.

(17) Destruction Methods. Destroy paper and non-paper COMSEC material by burning, shredding via NSA authorized devices, pulping, chopping, or pulverizing. Burning is normally only done outside the continental United States.

(a). Destroy non-paper COMSEC material by burning, chopping, pulverizing, or chemically altering until it is decomposed to such a degree that there is no possibility of reconstructing key, keying logic, or classified COMSEC information by physical, electrical, optical or other means.

(b). Magnetic or electronic storage and recording media are handled on an individual basis. Destroy magnetic tapes by disintegration or incineration. Destroy magnetic cores by incineration or smelting. Destroy magnetic disks and disc packs by removing the entire recording surface by means of emery wheel or sander, or send via Defense Courier Service to the National Security Agency Destruction Facility.

(c). Burning is the only means currently authorized for destroying diskettes that either are storing or have been used to store keying material. Destruction by shredding is not considered sufficient to ensure complete destruction of diskettes.

(d). See EKMS 704C LMD/KP Operator's Manual for destruction methods for keying material stored within the KP.

(18) Deployment. The MEF COMSEC Management Office (MCMO) deployment plan is established to increase the efficiency of the MCMO during contingencies. The plan provides guidelines on the organizational structure and use for each of the MCMO accounts and their employment. The mission of the MCMO is to provide I MEF units with a ready supply of appropriate, mission essential CMS material in support of the various Operational Plans (OPLANS).

(a). When a unit deploys, the EKMS account goes with the unit. It is only left behind as part of the Remain Behind Element (RBE) as described in this chapter. If the EKMS account is left behind an EKMS Manager must remain behind to run the account. Every six digit EKMS account requires an EKMS manager at all times.

(b). When a Marine Expeditionary Unit (MEU) goes on a training exercise as part of the MEU workup, the EKMS account either goes with the unit or stays behind. The EKMS account can not be locked up in a vault and left alone while the EKMS Manager and Alternates go off on a training exercise. The EKMS Manager or Alternates must always remain with the account.

(19) Joint COMSEC Management Office. The MCMO is a direct descendant of the Theater COMSEC Management Office (TCMO) that was activated during Desert Storm. The MCMO is designed to provide COMSEC support to the units in its parent MEF. If the decision is made to commit a joint command into a specific theater, support will be provided by the JCMO for all services in that theater. The Joint COMSEC Management Office (JCMO) is intended to provide EKMS support for a Joint Command.

(a). Marines assigned to the JCMO would be fully integrated into the JCMO; however the MCMO would continue to function as the ISIC and Controlling Authority for MEF EKMS material. In the event that the JCMO and MCMO are not co-located, the I MEF CE account would take over the duties for distribution of EKMS material to the entire MEF.

(20) Responsibilities of MCMO Accounts. First Marine Expeditionary Brigade Account. This account is held in a contingency status until the MEB is activated for deployment. Once the MEB is activated, the MCMO Cache account will transfer electronically all CMS material required by the MEB.

Depending on the expected length of the deployment, the MCMO Cache Account will transfer the current month plus either three or six months Reserve-On-Board (ROB), both ICP and specific AOR CMS material. While deployed, the MEB account will act as the ISIC for all accounts assigned to the MEB and will provide the necessary Inter-theater COMSEC Package (ICP) and AOR specific key to all subordinate units. The MCMO will provide for shipment of any additional CMS material required via the Defense Courier Service (DCS). The equipment and personnel to man the MEB account will come from the MCMO. This process also applies to the contingency accounts at each Major Subordinate Command and 9th Communication Battalion.

(a). I MEF CE Account. This is an active account that provides all EKMS material for the I MEF Command Element. When the entire MEF Command Element deploys, this account will deploy with it to provide all the required support. The MCMO Cache Account will transfer all required ICP and AOR specific material to this account. The CE account will transfer all RBE material to the MCMO Cache account for use at Camp Pendleton. If the JCMO is activated, and the MCMO becomes part of it, this account will take over the responsibility for distribution of CMS material. The equipment and personnel to man this account will come from the MCMO.

(b). MCMO Cache Account. This account will maintain sufficient quantities of all materials required to field the entire MEF at one time for contingency requirements. This account will hold all CMS (software) material for the MEF that will be needed for deployment or contingency operations, but not normally needed for routine training or operations in the Eastern Pacific Area. This account will also serve as the Controlling Authority for I MEF controlled CMS material, and as the senior ISIC CMS account for I MEF. This account will not deploy with the MEF. This account will become part of the I MEF at Camp Pendleton and provide support to both the deployed MEF and all remaining MEF elements located here at Camp Pendleton.

(21) EKMS Deployments Examples. Whenever a unit deploys it will take with it its EKMS account on deployment. It will not leave the EKMS account in garrison when it deploys. A Regionalization Deployment Plan has specific exceptions listed below

(a). Regionalization Deployment Plan. This plan requires prior planning. One or two EKMS accounts will be established within a defined geographical area (OCONUS) to support multiple units within a defined geographical area. The accounts will provide COMSEC support to forward units, the RBE and Replacement training cadre. Prior to providing support Memorandums of Agreement, Letters of Authorization, EKMS Acknowledgement Forms and all other required documentation must be completed with the servicing EKMS account.

(b). Commanding General (CG) First MARDIV, CG First MLG and CG Third MAW are responsible for providing pre-deployment guidance and assistance to subordinate commands with EKMS account. In addition to this order, ISICs may implement more stringent requirements.

(22) MEU Deployments. Thirty days prior to deployment, the MEU EKMS custodian will submit a request for keying material to the I MEF MCMO account. The MEU will normally deploy with the current month plus six months ROB.

(a). The MEU will also submit their itinerary and port visit schedule via formal record message to the local Defense Courier Service (DCS) Station in San Diego. This provides the DCS Couriers a location to ship

future or emergency material to. An example of this message can be found in enclosure (2) of this Order.

(b). Major Subordinate Elements (MSE) and all Detachments must identify and provide unique short titles and quantities of COMSEC material required for the deployment to the MEU EKMS manager.

(c). The parent command of MSEs and Detachments attached to the MEU will transfer all CCI items required for deployment, and any specific keying material to the MEU EKMS account. The MEU EKMS Manager will issue the gear back to the MSE's attached representatives as Local Elements. The exception to this is the detachment from Marine Special Operations Battalion.

(d). The transfer of this equipment and any related terminal specific COMSEC keying material to the MEU EKMS account does not bestow ownership to the MEU beyond the MEU deployment cycle. All items will be transferred back to the MSE no later than 60 days after the return of the MEU from deployment.

5. Command and Signal

(a) Command. This Order is applicable to all I MEF structure and functional roles are established as follows:

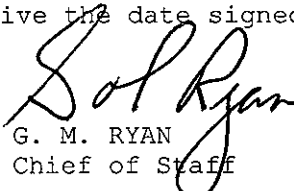
(1) Director for I MEF COMSEC Management Office. The requirements, administration, and resources sponsor for I MEF EKMS accounts.

(2) I MEF MCMO. Responsible for validating request for COMSEC material, providing guidance and oversight of subordinate EKMS accounts; maintaining positive custody, control and administration of COMSEC material in cache accounts; and, maintaining Marine Corps EKMS training center. Serve as ISIC for MSCs and MSEs.

(3) 1st MARDIV/1st MLG/3rd MAW. Responsible for validating providing guidance and oversight of subordinate EKMS accounts; maintaining positive custody, control and administration of COMSEC material in cache accounts. Serve as ISIC for Subordinate Commands (MSCs) and Subordinate Elements (MSEs).

(4) MEUs/Battalions/squadrons/Units. Responsible for maintaining positive custody, control and administration of COMSEC material in EKMS account including Local Elements (LEs).

(b). Signal. This order is effective the date signed.


G. M. RYAN
Chief of Staff

DISTRIBUTION: Electronically via the I MEF websites:
<http://www.i-mef.usmc.mil> and <http://www.imef.usmc.smil.mil>

COMSEC DEFINITIONS

Accounting Legend (AL) Code: A numeric code used in the COMSEC Material Control System (CMCS) to indicate the minimum accounting controls required for an item of accountable COMSEC material.

Accounting Number: A number assigned to an individual item of COMSEC material to simplify its handling and accounting. (NOTE: Also referred to as register or serial number.)

Advice and Assistance (A&A) Training Team: Worldwide network of CMS subject matter experts who provide training and assistance to personnel with COMSEC responsibilities.

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

AL 2: AL 2 COMSEC material is continuously accountable by quantity from production to destruction.

AL 3: AL 3 COMSEC material is locally accountable by accounting (register/serial) number after initial receipt.

AL 4: AL 4 COMSEC material is locally accountable by quantity after initial receipt.

AL 6: AL 6 COMSEC material is electronically generated and is continuously accountable to the COR by short title and accounting number from production to destruction.

AL 7: AL 7 COMSEC material is electronically generated and is accountable to the generation facility. All key transfers, including all subsequent transfers, must also be reported to the generating facility.

Amendment: A correction or change to a COMSEC publication.

Canister: Type of protective package used to contain and dispense in punched or printed tape form.

EKMS-1A: CMS Policy and Procedures Manual.

EKMS-3: CMS Inspection Manual.

EKMS-5: CMS Cryptographic Equipment Information/Guidance Manual.

EKMS-6: STU-III Policy and Procedures Manual.

CMS 16-1: Questionnaire and signature page for inventory reports. CMS-17: Used to record COMSEC material issued on local custody.

CMS-25: Single-copy segmented COMSEC keying material destruction report.

EKMS Account: An administrative entity, identified by a six-digit account number, responsible for maintaining accountability, custody and control of COMSEC material. (NOTE: A CMS account may also hold STU-III COMSEC material)

EKMS Clerk: Individuals assigned to assist custodian personnel in the execution of certain administrative duties associated with the management of a CMS account. (NOTE: Appointment of a CMS Clerk is at the discretion of the commanding officer/SCMSRO)

EKMS Custodian: Individual responsible for all actions associated with the receipt, handling, issue, safeguarding, accounting, and disposition of COMSEC material assigned to a command's CMS account.

EKMS User: Individual responsible for the proper security, control, accountability, and disposition of the COMSEC material placed in their charge. (NOTE: A CMS User may or may not have signed for COMSEC material)

EKMS Witness: Individual who assists custodian or user personnel in the proper execution of tasks related to the handling and safeguarding of COMSEC material (e.g., receipt, destruction, inventory, adherence to TPI handling requirements).

Communications Security (COMSEC): Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. government concerning national security, and to ensure the authenticity of such telecommunications. (NOTE: COMSEC includes crypto security, emission security, transmission security, and physical security of COMSEC material and COMSEC information)

Compromise: Disclosure of information or data to unauthorized person(s), or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

COMSEC Equipment: Equipment designed to provide security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor and, subsequently, by reconverting such information to its original form for authorized recipients; also, equipment designed specifically to aid in, or as an essential element of, the conversion process. (NOTE: COMSEC equipment includes crypto, crypto-ancillary, crypto-production, and authentication equipment)

COMSEC Incident: Any uninvestigated or unevaluated occurrence that has a potential to jeopardize the security of COMSEC material or the secure transmission of classified or sensitive government information; or any investigated or evaluated occurrence that has been determined as not jeopardizing the security of COMSEC material or the secure transmission of classified or sensitive government information. (NOTE: COMSEC incidents and insecurities are categorized as cryptographic, personnel, or physical.)

Data Transfer Device (DTD): A common fill device used to store and distribute electronic key.

Naval Communications Security Material System (NCMS): Administers DON CMS program and functions as SERVAUTH for DON EKMS Accounts. Serves as COR/Tier 1 for Legacy Tier 2 Accounts.

EKMS 704C: Operators manual for the EKMS LMD/KP.

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

Electrical Transaction Report (ETR): Formatted data fields used to report CMS transactions (e.g., receipt, transfer).

Fill Device (FD): Any one of a family of devices developed to read in, transfer, or store key. Current FDs are: KOI-18, KYK-13, KYX-15, KIK-18A, and DTD (AN/CYZ-10).

FIREFLY: Key management protocol based on public key cryptography.

Firefly Credentials: FIREFLY exchange information required by another element/entity in order for both elements/entities to cooperatively generate the same session key. (NOTE: Credentials are not key and therefore do not have a crypto period. Credentials do have an expiration date - one month from the first use of the credential or the end of the associated FIREFLY's crypto period, whichever comes first).

Highest Classification Indicator (HCI): Used to determine the highest classification of COMSEC material that an account may hold.

Immediate Superior in Command (ISIC): Command responsible for the administrative oversight of all CMS matters for their subordinate commands.

KAM: Cryptographic Operational Maintenance Manual or maintenance manual for a cryptosystem.

KAO: Cryptographic Operational Operating Manual or operating instruction manual for a cryptosystem.

Keying Material: A type of COMSEC item in physical or non-physical form which supplies either encoding means for manual and auto-manual cryptosystems or key for matching cryptosystems.

Page check: Verification that all pages of a publication or technical manual are accounted.

Short Title: A series of letters and/or numbers (e.g., KG-84, USKAT 2333), used for brevity and assigned to certain COMSEC materials to facilitate handling, accounting, and control.

Two-Person Integrity (TPI): A system of handling and storing designed to prevent single-person access to certain COMSEC keying material.

Zeroize: To remove or eliminate the key from a crypto-equipment or FD.

OFFICIAL CORRESPONDENCE

APPOINTMENT LETTER

From: Commanding Officer or Staff CMS Responsibility Officer (SCMSRO)

To: (Rank, Name, SSN (last 4 digits))

Subj: LETTER/MEMORANDUM OF APPOINTMENT

Ref: (a) EKMS-1 (Series)

1. In accordance with reference (a), you are hereby appointed as (EKMS Manager, Alternate EKMS Manager, Local Element (Issuing), STU III User Representative, LMD UNIX System Administrator, or COMSEC Clerk) for this command.

2. EKMS account number: _____.

3. EKMS Manager course (V-4C-0013) completed on (YYMMDD) at Name/Location of EKMS school attended.

4. Security clearance: _____.

5. Following designation, requirements contained in Article 415 (as applicable) of the reference are waived:

a. _____

b. _____

(identify authority for and specific requirement(s) waived; if no requirements waived, indicate N/A)

Signature of Commanding Officer
or Staff CMS Responsible Officer

CMS RESPONSIBILITY ACKNOWLEDGEMENT FORM

From: _____
(Rank/Rate, Full Name, SSN, and Command of CMS User)
To: (EKMS Manager or LE Custodian), _____
(Name of Command)

Subj; CMS RESPONSIBILITY ACKNOWLEDGEMENT

Ref: (a) EKMS 1 Series and/or the local command instruction governing the handling, accountability, and disposition of COMSEC material.

1. I hereby acknowledge that I have read and understand reference (a).
2. I assume full responsibility for the proper handling, storage, inventorying, accounting, and disposition of the COMSEC material held in my custody and/or used by me.
3. I have received a copy of reference (a) from the (EKMS Manager or LE Custodian). If at any time I am in doubt as to the proper handling of COMSEC material that I am responsible for, I will immediately contact the EKMS Manager and request advice.
4. Before extended departure from the command (i.e., permanent transfer, or leave/TAD/TDY in excess of 60 days) I will report to the (CMS or LE Custodian) and be relieved of responsibility for all COMSEC material that I have signed for.

Signature
Date

NOTE: 1. Every CMS User and/or person to who COMSEC material is issued must complete the above CMS Responsibility Acknowledge Form. This requirement does not apply to individuals who access GPS key via the TAMPS for loading into aircraft.

2. This form will be reproduced locally and the required information will be typed or printed in black or blue-black ink.

3. Custodians/LE Custodian will retain this form in his/her Chronological File for a period of 90 days after the date an individual has been relieved of responsibility for COMSEC material that he/she signed for.

FORM 10

Date DDMMYY

From: Commanding Officer or Staff CMS Responsible Officer
To: EKMS Manager, Account #

Subj: AUTHORIZATION TO RECEIPT FOR AND COURIER COMSEC MATERIAL

Ref: (a) EKMS-1 Series

1. Per reference (a), the below named individuals are authorized to receipt for and to courier COMSEC material:

<u>GRADE</u>	<u>NAME</u>	<u>SSN(last four)</u>	<u>CLEARANCE</u>
--------------	-------------	-----------------------	------------------

2. This letter supersedes all previous letters.

Signature of Commanding Officer or
Staff CMS Responsible Officer

INCIDENTAL USERS ACKNOWLEDGEMENT STATEMENT

I understand that on occasion I may be required to operate keyed radio equipment as an incidental operator. I have been properly indoctrinated and fully understand the sensitivity of COMSEC material, the rules for safeguarding such material and the rules for reporting COMSEC incidents.

Name/Rank _____ SSN (Last 4) _____ Signature _____ Date _____

DEFENSE COURIER SERVICE (DCS) CHANGE OF ADDRESS REQUEST

FROM: EKMS MANAGER
TO: dc_sdni_all@navy.mil
CC: ISIC
SUBJECT: DCS CHANGE OF ADDRESS REQUEST
EMAIL TEXT: REQUEST ALL DCS SHIPMENTS FOR 299326-BH03/ HKR016 DCS SN 030 CG I
MEF G6 BE RE-ROUTED AND CHANGED TO 299326-SN04/ HKS237 DCS SN 030 (DCS SAN
DIEGO) EFFECTIVE 31 JULY 2008.
REQUEST DCS BAHRAIN FAX DCS FORM "USTRANSCOM IMT 10" TO DCS SAN DIEGO SN04.

NOTE: REQUEST FOR CHANGE OF ADDRESS WILL BE SENT TO DSC BULK EMAIL ACCOUNT
"dc_sdni_all@navy.mil" via NIPERNET. EKMS ACCOUNTS ARE REQUIRED TO SUBMIT
REQUEST FOR POST DEPLOYMENT AND RE-DEPLOYMENT DCS SUPPORT.

OTAR/OTAT LOGS

GENERATING STATION OTAR AND OTAT LOGS

The form on the next page is for your use to record monthly OTAR/OTAT transactions. Local reproduction of this form is authorized.

Block Completion is identified, as follows:

1. KEY SOURCE.
2. SHORT TITLE.
3. CLASS (Classification of material sent/received).
4. CA (Controlling Authority of material sent/received).
5. EFF PD (Effective period of material).
6. STORAGE POSITION AND FILL DEVICE SERIAL NUMBER.
7. CIRCUIT IDENTIFICATION (IDO TRANSMITTED OVER RECEIVED).
(Identify circuit used to transmit or receive)
8. DATE/TIME OF TRANSMISSION.
9. RECEIVING STATION(S).
10. ZEROIZED DATE/TIME.
11. INITIALS (Initials of the two personnel that zeroized the transaction).

GENERATING STATION OTAROTAT LOG FOR THE MONTH OF

[illegible]

CONFIDENTIAL (When filled in)

RELAYING/RECEIVING STATION OVER-THE-AIR TRANSFER (OTAT LOG)

The form on the next page is for your use to record monthly OTAT transactions. Local reproduction of this form is authorized.

Block Completion is identified as follows:

1. KEY IDENTIFICATION (ID) SHORT TITLE.
2. CA (Controlling Authority of material sent/received).
3. CLASS (Classification of material sent/received).
4. CIRCUIT KEY INTENDED FOR (Identify the system/Purpose).
5. EFF PD (Effective period of material).
6. DATE/TIME RECEIPT (R) TRANSMISSION (T).
7. CIRCUIT IDENTIFICATION TRANSMITTED OVER RECEIVED.
8. STORAGE POSITION AND FILL DEVICE SERIAL NO.
9. ZEROIZED DATE/TIME.
10. INITIALS (Initials of the two personnel that zeroized the key if the key is Top Secret).

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

[illegible]

CONFIDENTIAL (When filled in)

CHECK LIST

EKMS MANAGERS TURNOVER CHECKLIST

- ___ 1. Conduct Change of EKMS Manager Inventory. (EKMS-1 Art 766)
- ___ 2. Verify that the latest semi-annual inventory has been reported to the COR. (EKMS-1 Art 766 b.1)
- ___ 3. Review the results of the last EKMS inspection. Ensure discrepancies have been corrected. Verify that inspection has occurred within the past 24 months. Contact your ISIC if past 24 months. (EKMS 3 series)
- ___ 4. Review results of last CMS A&A 18 month training visit as required. Ensure discrepancies have been corrected. (EKMS-1 Art. 325)
- ___ 5. Verify all access lists, authorization to handle COMSEC material list, EKMS responsibility acknowledgement forms, and personnel security clearance data is up to date. (EKMS-1 Annex K)
- ___ 6. Review all Letters of Agreement. (EKMS-1 Annex K)
- ___ 7. Review all Commanding Officer Spot Checks. (EKMS-1 Annex D)
- ___ 8. Have your Command Authority (CA) assign you key ordering privileges as the User Representative (UR). In some commands the CA and UR may be the same. (EKMS-1 Annex AB, EKMS 702.01)
- ___ 9. Update CMS Form 1. (EKMS-1 Annex H)
- ___ 10. Update DCS Form 10. (EKMS-1 Art. 751.b)
- ___ 11. Update EKMS Manager and Alternate Letter of Appointment. (EKMS-1 Art 425)
- ___ 12. Update Common Account Data (CAD). (EKMS-1 Art 435, EKMS 704)
- ___ 13. Review DTD audit trail data and DTD audit log. (EKMS-1 Annex Y, paragraph 17)
- ___ 14. Notify your Immediate Superior in Command (ISIC) that you are assuming the duties as EKMS Manager.
- ___ 15. Review command Standard Operating Procedures for EKMS accounts. (EKMS-1 Art 550.i)
- ___ 16. Review command Emergency Action Plan (EAP) and Emergency Protection Plan. (EKMS-1 Annex L)
- ___ 17. Review commands SF-700's. (EKMS-1 Art 515)
- ___ 18. Ensure Command has 4 REINIT 1 and 4 REINIT 2 Keys.

(EKMS-1A Art 1185 d)

____ 19. Register as LMD/KP System Administrator. Ensure Primary Alternate is registered as LMD/KP system administrator. (EKMS-1 Annex W Para 7)

____ 20. Verify date of last back-up (daily). (EKMS-1 art 718.d.)

____ 21. Ensure all administrators and operators have KP CIK and KP Pins. Recommend each have one (1) back-up. (EKMS-1 Annex W Para 10)

____ 22. Verify date of last root back-up (every 30 days). (EKMS-1 art 718)

____ 23. Verify date of last Archive (every six months). (EKMS-1 Annex W para 10.s.)

____ 24. Verify date of last changeover (every 3 months). (EKMS-1 Annex W para 10.t.)

____ 25. Verify date of last KP rekey (every 12 months). (EKMS-1 Annex W para 10.u.)

____ 26. Verify date of last KP recertification (3 years).
(EKMS-1 Art 1185 e)

____ 27. Schedule CMS A&A Training Visit as required.

****Maintain a copy of this Check List in your Chronological Files****

Outgoing EKMS Manager

Incoming EKMS Manager

Note: It is recommended that the incoming and outgoing EKMS Managers do a self check using EKMS-3 (series) to ensure the account is in order prior to turnover.

EKMS MANAGERS PRE-DEPLOYMENT CHECKLIST

- ___ 1. Work with Communication Section and Local Elements to determine deployed COMSEC hardware and software support requirements. You must derive a list of COMSEC key required in country so that you can release your Modification of Allowance message. Your embark plan will depend on unit allocations and requirements. The items in **BOLD** MUST be escorted and may NOT be sent with bulk embarked items due to security.
- ___ 2. Determine embarkation requirements. A six-digit account should plan on bringing the following:
- ___ a. **Entire LMD system to include LMD CPU, monitor, keyboard, Mouse, A/B switch, HP LaserJet 6 printer, UPS, and associated cables.**
 - ___ b. **KP with re-init 1 and 2 keys and sysadmin keys.**
 - ___ c. **STU-III/STE with EKMS key loaded or ready.**
 - ___ d. EKMS Manager's CYZ-10 and KOI-18.
 - ___ e. Security Containers.
 - ___ f. **LCMS backup tapes to include spares.**
 - ___ g. (2) spare toner cartridges for the HP LMD printer.
 - ___ h. EKMS Pubs (can be electronic but recommend hard copy of EKMS-1).
 - ___ i. **EKMS Files to include (Chronological, Correspondence, Directives, General Message File, and Local Custody files).**
 - ___ j. Spare batteries for the CYZ-10, STU phones, TACLANES and KIV-7's.
 - ___ k. Multi-Function printer/copier/fax/scanner. If not, bring a scanner at minimum.
 - ___ l. SF-700 Forms with lamination and aluminum foil.
 - ___ m. X-07/8/9 combo instructions and change key.
 - ___ n. Greenleaf combo locks.
 - ___ o. General office supplies (30 days worth).
 - ___ p. Operational STU/STE key.
 - ___ q. Heavy-duty power down-converters.
 - ___ r. Classification stamps, etc...
 - ___ s. Ammo can for burn destruction.

_____t. LMD Hard Drive

_____u. Clipboard (for inventory)

_____ 3. Inform your S-4/Embarkation rep that you will be escorting classified material. They will want to know the amount and type of containers and the name of the escort(s). Normally, the EKMS Manager and Alternate serve as escorts (or "pallet riders") along with any other properly cleared and authorized personnel.

_____ 4. If you have been designated as an account that will provide key to users, release your MOA reflecting the key required by your Local Elements. This should include any key required by attached units you will support. Contact the EKMS account manager you are relieving in country to determine key requirements in addition to your LE's.

_____ 5. Draft and have signed, all courier documents required for the "pallet riders" and escorts.

_____ 6. Make arrangements with your ISIC to transfer all physical key material you do not want to transport.

_____ 7. If your command has a "Remain Behind Element", appoint and train a LE custodian. When able, issue RBE CCI to this element.

_____ 8. Maintain copies of all embarkation packing lists containing CCI. Insure that NO CCI is keyed prior to embarkation.

_____ 9. Inform your servicing DCS station that your account is deploying and that you want your material delivered to DCS Bahrain.

_____ 10. Update your CMS Form 1 with I MEF MCMO.

_____ 11. If your Key Processor is close to its re-cert date, contact CMIO about receiving a new one prior to your deployment. You want to do the REINIT prior deploying so that you don't have to do it in country.

_____ 12. Request a KP rekey within one month of deployment. Post own credentials once rekey has been received from Central Facility.

_____ 13. Download and process from the x.400 Directory Services, all the credentials from accounts you will work with while deployed.

_____ 14. Contact the EKMS account manager for the unit you will be relieving in Iraq for information on:

_____a. Crypto Key being used.

_____b. Name of each Local Element supported and type of support.

_____c. Qty/Type of security containers that will remain in place.

_____d. Information on EKMS vault/facility/shelter.

- ____e. LMD Connectivity.
 - ____f. INMARSAT turnover.
 - ____g. Projected departure dates for EKMS Mangers and LE's.
 - ____h. Crypto key that will be transferred to your account.
 - ____i. Iridium phones that will be transferred to your account.
- ____ 15. Formulate "EKMS escort plan".
- ____a. Will you pallet ride with all EKMS equipment?
 - ____b. Prepare to embark your LMD hard drive, REINIT and sysadmin keys, backup tapes, Key Processor, and classified pubs and EKMS files.
 - ____c. Train and Brief escorts.
- ____ 16. Activate service and perform operational checks on INMARSAT system if using. POC for INMARSAT related issues at HQMC C4 is LtCol Jeff Nelson, DSN 223-3468.
- ____ 17. Contact Mr. Sylvan at NCMS N3 about receiving your MIC3 via SIPRNET. DSN 857-9711. Important due to connectivity issues.
- ____ 18. Perform one last root, /u, and LCMS database backup prior to packing and label accordingly.
- ____ 19. Print one copy of AIS and keep in the "deployment folder" that you keep with you.
- ____ 20. Ensure that you, the EKMS reps from your LE's and possibly your CMR RO's are on the advance party.
- ____ 21. Backup your MS Outlook .pst files, Internet Explorer favorites, and EKMS documents to CD-ROM for both SIPR and NIPR accounts.

END OF YEAR PROCEDURES

All EKMS accounts are required to keep the following files; Chronological File, Correspondence/Message and Directives File General Message File and Local Custody File. See articles 706, 709, 712 of ref (a) for contents of these files.

Annex S, of Ref (a), retention periods for COMSEC files, records, and logs. The general rule is that all files are kept for a minimum of 2 years with the main exception of archived data which is kept for a minimum of 3 years.

To ensure the maintenance and accountability of COMSEC material within I MEF, all I MEF EKMS will follow the below end of year procedures to be completed by each account by the 15th of January of every year:

A. Transaction status log; verify all transaction for the previous 12 months have been reconciled, no pending transaction. See EKMS 704 c chapter 4 (page 4-4). For example: select display then pending between. This will show you the "transaction status" box where you enter the "starting date" of 20050101 and the "end date" of 20051231. Clicks accept.

B. Archive your hard copy files, i.e. chronological, correspondence, general message, etc.. Ensure that all SF-153's are filled out correctly.

C. Verify all access lists, authorization to handle COMSEC material list, responsibility acknowledgement forms.

D. Review all Letters of Agreement.

E. Update CMS Form 1.

F. Update DCS Form 10.

G. Updates EKMS manager and alternate letters of appointment.

H. Update common account data (CAD).

I. Review and update command emergency action plan (EAP).

J. Verify date of last archive.

K. Verify date of last KP rekey.

L. Verify date of last KP recertification.

M. Reinitialize dtd CIK.

N. Review COMSEC holdings to ensure continuing need for quantity and types of material held.

O. Carry forward to new files any general msg that is still in force for the next year.

Note: All I MEF accounts will verify to their ISIC by 30 Jan of each year, via email or naval msg, that the above has been completed.

Procedures For routine Modification of COMSEC Allowance

PROCEDURES FOR ROUTINE MOD OF AN ACCOUNT ALLOWANCE FOR COMSEC KEYING MATERIAL

The below format is to be used to acquire COMSEC keying material not previously authorized for receipt by the account and for routine modification of an accounts allowance of authorized holdings of COMSEC keymat. Where Information for a particular short title is not applicable, insert N/A. CONAUTH approval must be obtained. A minimum of 60 days lead time is required. Request should be addressed as follows:

TO: NEXT SENIOR FLAG LEVEL COMMAND/ISIC
 CC: CMC WASHINGTON DC C4 IA
 CHAIN OF COMMAND
 THE APPLICABLE COR
 CONAUTH (IF MULTIPLE CONAUTH, LIST ALL PLA's)
 HQ USPACOM J6 (FOR JCMO, CENTCOM OR PACOM KEYMAT)
 NCMS WASHINGTON DC
 CMIO NORFOLK

SUBJ: ROUTINE MODIFICATION IN COMSEC KEYMAT ALLOWANCE
 NOTE: EACH USMC FLAG LEVEL COMMAND (I.E., DIV, MAW, MLG AND MEF) MUST REVIEW AND FORWARD THEIR ENDORSEMENTS UP THE CHAIN OF COMMAND TO COMMARFORPAC. MULTIPLE SHORT TITLES MAY BE COMBINED AND SUBMITTED IN A SINGLE MESSAGE. EACH SHORT TITLE MUST BE ASSIGNED A SEPARATE PARAGRAPH AND THE ACTION ADDRESSEE FOR EACH SHORT TITLE MUST BE CLEARLY IDENTIFIED (E.G., 1.FOR NCMS, 2.FOR JCMO, 3.FOR COMPACFLT) IN THE CASE OF MULTIPLE ACTION ADDRESSEES.

REQUEST WILL BE IN THE BELOW FORMAT:

1. FOR: NAME OF CONAUTH
- A. EKMS ACCOUNT NUMBER, COMMAND NAME AND HCI.
- B. SHORT TITLE
- C. PERMANENT OR TEMPORARY SPECIFY DATES IN YYYY FORMAT
 FOR TEMPORARY (E.G., 9906 - 9910)
- D. INCREASE OR DECREASE, QUANTITY AND JUSTIFICATION
- E. PRESENT APPROVED ALLOWANCE
- F. DATE MATERIAL NEEDED
- G. NAME OF ISIC
- H. SERVICING DCS STATION
- I. POC AND PHONE NUMBER (S)

ROUTINE MODIFICATION OF AN ACCOUNT ALLOWANCE FOR COMSEC EQUIPMENT AND RELATED DEVICES

The below format is to be used to transfer COMSEC equipment (T/E ITEMS) and related devices between USMC accounts subordinate to I MEF. This is not for requesting disposition instruction. Commands will forward request up their Chain-of-Command (COC) to the next senior flag level (I.E., DIV, MAW, MLG,) for authorization or endorsement. Where Information for a particular short title is not applicable, insert N/A. COMSEC equipment and related devices(S) request should be addressed as follows:

TO: NEXT SENIOR FLAG LEVEL COMMAND/ISIC
 CC: CMC WASHINGTON DC C4 IA
 CHAIN OF COMMAND
 COMMARCORSYSCOM QUANTICO VA CINS
 NCMS WASHINGTON DC
 CMIO NORFOLK VA
 CSLA TIER 1

SUBJ: ROUTINE MODIFICATION OF ALLOWANCE FOR COMSEC EQUIPMENT AND RELATED DEVICES

REQUEST WILL BE IN THE BELOW FORMAT:

1. EKMS ACCOUNT NUMBER, COMMAND NAME AND HCI
 - A. SHORT TITLE
 - B. PERMANENT OR TEMPORARY
 - C. INCREASE OR DECREASE, QUANTITY, AND JUSTIFICATION
 (LIST ACCOUNT NUMBER, AND NAME OF COMMAND RECEIVING THE EQUIPMENT)
 - D. PRESENT APPROVED T/E ALLOWANCE
 - E. DATE MATERIAL NEEDED
 - F. NAME OF ISIC
 - G. SERVICING DCS STATION
 - H. POC AND PHONE NUMBER(S)
 - I. QTY ON HAND AND DEFICIENT OR EXCESS AMOUNT

NOTES: MCO 4400.172 delineates USMC procedures and responsibilities for requesting a Modification of Allowance (MOA) for COMSEC Tables of Equipment (T/E) allowances. Quantities listed in routine modification of COMSEC equipment allowance request must reflect the quantity listed in T/E allowances. Marine aviation organizations whose COMSEC equipment is not authorized by and established in a T/E and is in direct support of "Blue Dollar" Navy must follow procedures delineated for "Navy Commands". Information on transferring NON T/E items can be found in the EKMS-1a and EKMS.