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

I MEFO 2281.1A
G-6
FEB 7 2018

I MARINE EXPEDITIONARY FORCE ORDER 2281.1A

From: Commanding General
To: Distribution List

Subj: COMMUNICATIONS SECURITY STANDARD OPERATING PROCEDURES

Encl: (1) I MEFO 2281.1A

1. Situation. This change is issued to transmit the following:

a. To capture the renaming of the Electronic Key Management System (EKMS), to the Key Management Infrastructure (KMI).

b. Removal of antiquated terminology and outdated procedures.

c. To outline I MEF specific guidance as it pertains to operational roles within KMI.

2. Execution. Throughout this Order, the term "EKMS" is still used because the naval policy manuals regarding communications security are still referred to as the "EKMS" series manuals.

3. Summary of Change. At the direction of the Chief of Staff, this revision has been fully staffed and all administrative errors and inputs have been corrected or consolidated. These changes ensure the most updated information is disseminated to the I MEF Command Element, Major Subordinate Commands and Elements.

4. Filing Instructions. File this change transmittal immediately behind the signature page of the basic Order.

LEWIS A. CRAPAROTTA

DISTRIBUTION LIST: I, II

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

I MEFO 2281.1A
G-6 MCMO

FEB 7 2018

I MARINE EXPEDITIONARY FORCE ORDER 2281.1A

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

Subj: COMMUNICATIONS SECURITY STANDING OPERATING PROCEDURES

Ref: (a) EKMS 1 (Series) (Supp-1)
(b) EKMS 3 (Series)
(c) EKMS 5 (Series)
(d) SECNAVINST 5510.36A
(e) OPNAVINST C5510.93F
(f) DoDD 8570.01
(g) MCO P5510.18A
(h) MCO 5530.14A
(i) MCO 2281.1A
(j) COMSEC Management for Commanding Officer's Handbook

Encl: (1) COMSEC Definitions
(2) Cryptographic Access Certification and Termination (SD-572)
(3) Sample Letter/Memorandum of Appointment
(4) KOAM Turnover Checklist
(5) KOAM Pre-deployment Checklist
(6) End of Year Procedures
(7) Procedures for Routine Modification of COMSEC Allowance
(8) Defense Courier Service (DCS) Change of Address Request
(9) Disposition Instructions
(10) CCI Transfer/Receipt Checklist
(11) Required Accounting and Control Procedures
(12) Deployment Plan

1. Situation. Communication Security (COMSEC), also known as Key Management Infrastructure (KMI) is the all-encompassing key management system providing the capability for generation, distribution, destruction, and management of electronic cryptographic keying material (keymat), as well as the management of physical keymat and non-keymat related COMSEC items such as: communications equipment, documents, firmware, or software that embody or describe cryptographic logic and other items that perform COMSEC functions. The proper handling, accounting, safeguarding, and disposition of COMSEC material is vital in protecting information which if compromised, could jeopardize National Security or result in endangering forward deployed elements.

2. Cancellation. I MEFO 2281.1.

3. Mission. To supplement the references and establish specific I Marine Expeditionary Force (MEF) COMSEC policy and procedures concerning the appropriate handling of COMSEC material and the proper management of COMSEC accounts within I MEF.

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. To mitigate COMSEC vulnerabilities, I MEF commands with KMI Operating Accounts (KOA) are to ensure that control of COMSEC material and training of all personnel in receipt of COMSEC materials is in accordance with this order and all applicable references.

(2) Concept of Operations. Strict adherence to national, Department of the Navy, and Marine Corps COMSEC policies shall be applied for the protection of COMSEC material. Therefore, the I MEF COMSEC Management Office (MCMO) is responsible to the Commanding General for COMSEC planning and operations of Major Subordinate Commands (MSC), Immediate Superiors In Command (ISIC), and elements of I MEF. The MCMO will facilitate periodic training for all I MEF COMSEC account managers and ISICs to discuss policy changes, and identify current trends that effect mission accomplishment. Additionally the MCMO will manage an inspection program to ensure compliance with established doctrine.

b. Subordinate Element Missions

(1) MEF COMSEC Management Office shall:

(a) Be responsible to the Commanding General for the oversight and management of the I MEF COMSEC Program.

(b) Maintain a Military Occupational Specialty (MOS) producing COMSEC Material Systems (CMS) training facility to provide basic entry level certification to newly appointed KMI Operating Account Managers (KOAM).

(2) Major Subordinate Command Immediate Superiors In Command shall:

(a) Be responsible to the MSC Commanding General for the oversight and management of their respective COMSEC Program.

(b) Maintain COR Audit program for your respective MSC.

(3) Commanding Officers (CO) and Officers-in-Charge (OIC). The CO is responsible for properly administering their command's COMSEC/KMI account and ensuring compliance with references (a) through (j). Reference (j) is written specifically for CO's and contains a CMS/KMI account assurance checklist for use in assessing command compliance. Throughout this Order, responsibilities applicable to the CO and OIC apply equally to the Staff CMS Responsibility Officer (SCMSRO). CO's and OICs shall:

(a) Appoint qualified individuals in writing as Primary KOAM, Alternates, Simple Key Loader (SKL) Site Security Officer (SSO), Secure Terminal Equipment Terminal Privilege Authority (TPA), Token Security Officer (TSO), Product Requester (PR), Client Platform Administrator (CPA), Client Platform Security Officer (CPSO), Device Registration Manager (DRM), Device Local Type 1 Registration Authority (DLT1RA), Personnel Local Type 1 Registration Authority (PLT1RA) users and Account Clerk as outlined in reference (a).

(b) Establish a list of personnel authorized access to COMSEC material.

(c) Ensure COMSEC incident reports are promptly and accurately submitted to appropriate officials, including the I MEF G-6, as outlined in reference (a).

(d) Ensure Primary and Alternate KOAMs meet the below requirements, in addition to requirements listed in reference (f):

1. Primary and Alternate KOAMs must be school trained before executing duties.

2. Primary KOAMs must be in the grade of E-6 or above, civilian employees must be GS-7 or above. Alternate KOAM's must be in the grade of E-5 or above, civilian employees must be GS-6 or above.

3. Primary and Alternate KOAMs will manage only one KMI account at a time or provide approved waiver from Naval Communications Security Material System (NCMS).

(e) The CO will conduct Spot Checks provided in reference (j). 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, one per quarter.

(4) 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, O-4 Select, GS-12, or above).

(5) Immediate Superior in Command (ISIC). The ISIC is responsible for the administrative oversight of all COMSEC matters for their subordinate commands. ISICs shall:

(a) Validate the operational requirement for the KMI account.

(b) Determine COMSEC material allowance requirements and, when required, obtain controlling authority authorizations per reference (a).

(c) Ensure Physical Security Surveys are conducted per references (g) and (h). ISIC's will authorize a facility to hold COMSEC material at a minimum of every 12 months during the COR Audit.

(d) Conduct COR Audits. All I MEF COMSEC accounts must receive an unannounced COR Audit once every 12 months. Ensure copies of reports are forwarded to Headquarters Marine Corps C4 Information Assurance (IA) and NCMS Command via the chain of command.

(e) Review and retain COMSEC records pending receipt of NCMS notice of reconciliation upon account disestablishment.

(6) Primary KOAM. Primary KOAMs shall be designated in writing by the CO. They will manage COMSEC material issued to the command's KMI account. The Primary KOAM is not required to have a 0681 occupational specialty. The Primary KOAM is the CO's primary advisor on matters concerning the security and handling of COMSEC material and associated records and reports.

(7) Alternate KOAM. Alternate KOAMs shall be designated in writing by the CO. They are responsible for assisting the Primary KOAM in the performance of their duties and assuming the duties of the Primary KOAM in their absence. Alternate KOAMs equally share responsibility for the proper management and administration of the KMI account with the Primary KOAM.

(8) KOA Clerk. KOA Clerks are responsible for assisting the Primary and Alternate KOAMs with routine administrative matters. Appointment of a KOA Clerk is not mandatory. KOA Clerks will not be granted access to COMSEC material.

(9) COMSEC User. 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 documents. Users must comply with the procedures for the handling and accountability of COMSEC material placed in their charge.

(10) COMSEC 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 access to keying material in writing.

(11) Site Security Officer (SSO). The AN/PYQ-10 (Simple Key Loader) and/or KIK-11 (Tactical Key Loader) audit trails must be reviewed monthly and 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 KOAM he/she must be designated in writing by the CO/SCMSRO as an authorized SSO/Supervisory user.

5. Administration/Logistics. COMSEC Account Managers subordinate to the I MEF command structure are required to maintain a copy of this order in their Directives File. Submit all recommendations for changes to this order to the I MEF, G-6 MCMO Director via the appropriate COMSEC chain of command. For the purposes of this order, the terms "COMSEC", "CMS", and "KMI" are used interchangeably.

6. Command and Signal

a. Command. This Order is applicable to the I MEF Total Force. All I MEF commands with a KOA, and those commands that provide oversight, shall review and comply with this Order.

b. Signal. This Order is effective the date signed.

LEWIS A. CRAPAROTTA

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.)

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 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.

Central Office of Record (COR): A central office which keeps records of all accountable COMSEC material held by elements subject to its oversight.

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

COR Audit Teams: Worldwide network of COMSEC subject matter experts established to provide assistance and training to personnel assigned COMSEC responsibilities.

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 encrypting information to a form unintelligible to an unauthorized interceptor and, subsequently, by un-encrypting such information to its original form for authorized recipients; also, equipment designed specifically to aid in, or as an essential element of, the encryption 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.)

EKMS-1 (Series): CMS Policy and Procedures Manual.

EKMS-3 (Series): CMS Inspection Manual.

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

Fill Device (FD): Any one of a family of devices developed to read in, transfer, or store key. Current FDs are: Simple Key Loader (SKL) and Tactical Key Loader (TKL).

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.

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

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

Key Management Infrastructure (KMI): All parts, computer hardware, firmware, software, and other equipment and its documentation; facilities that house the equipment and related functions; and companion standards, policies, procedures and doctrine, that form the system that manages and supports the ordering and delivery of cryptographic material and related information products and services to users.

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.

KMI Operating Account (KOA): An administrative entity, identified by a six-digit account number, responsible for maintaining accountability, custody and control of COMSEC material.

KOA Manager: The management role responsible for the operation of one or more KOAs (i.e., manages distribution of COMSEC keying material to the ECUs, fill devices, and AKPs that are assigned to the manager's KOA).

Local Element: Sections that are separate units or commands that require COMSEC material and function essentially as sub-accounts of a numbered CMS account. Local elements are managed similarly to a CMS account except they are not assigned a CMS account number and normally receive their COMSEC material from a parent CMS account.

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

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.

FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE: ANY MISUSE OR UNAUTHORIZED DISCLOSURE MAY RESULT IN BOTH CIVIL AND CRIMINAL PENALTIES.

CRYPTOGRAPHIC ACCESS CERTIFICATION AND TERMINATION

PRIVACY ACT STATEMENT

AUTHORITY: EO 9397, EO 12333, and EO 12356.
PRINCIPAL PURPOSE(S): To identify the individual and when necessary to certify access to classified cryptographic information.
ROUTINE USE(S): None.
DISCLOSURE: Voluntary; however, failure to provide complete information may delay certification and in some cases prevent original access to classified cryptographic information.

INSTRUCTIONS

Section I of this certification must be executed before an individual may be granted access to classified cryptographic information.

Section II will be executed when the individual no longer requires such access.

Until cryptographic access is terminated and Section II is completed, the cryptographic access granting official shall maintain the certificate in a legal file system, which will permit expeditious retrieval. Further retention of the certificate will be as specified by the DoD Component record schedules.

SECTION I - AUTHORIZATION FOR ACCESS TO CLASSIFIED CRYPTOGRAPHIC INFORMATION

a. I understand that I am being granted access to classified cryptographic information. I understand that being granted access to this information involves me in a position of special trust and confidence concerning matters of national security. I hereby acknowledge that I have been briefed concerning my obligations with respect to such access.

b. I understand that safeguarding classified cryptographic information is of the utmost importance and that the loss or compromise of such information could cause serious or exceptionally grave damage to the national security of the United States. I understand that I am obligated to protect classified cryptographic information and I have been instructed in the special nature of this information and the reasons for the protection of such information. I agree to comply with any special instructions issued by my department or agency regarding unofficial foreign travel or contacts with foreign nationals.

c. I acknowledge that I may be subject to a non-lifestyle, counterintelligence scope polygraph examination to be administered in accordance with DoD Directive 5210.48 and applicable law.

d. I understand fully the information presented during the briefing I have received. I have read this certificate and my questions, if any, have been satisfactorily answered. I acknowledge that the briefing officer has made available to me the provisions of Title 18, United States Code, Sections 641, 793, 794, 798, and 952. I understand that if I willfully disclose to any unauthorized person any of the U.S. classified cryptographic information to which I might have access, I may be subject to prosecution under the Uniform Code of Military Justice (UCMJ) and/or the criminal laws of the United States as appropriate. I understand and accept that unless I am released in writing by an authorized representative of , the terms of this certificate and my obligation to protect all classified cryptographic information to which I may have access, apply during the time of my access and at all times thereafter.

ACCESS GRANTED THIS _____ DAY OF _____ , _____

1. EMPLOYEE - DO NOT EMAIL THIS FORM WITH SSN FILLED IN!!!

a. SIGNATURE	b. NAME (Last, First, Middle Initial)	c. GRADE/RANK/RATING	d. SSN - Pen only!!!

2. ADMINISTERING OFFICIAL

a. SIGNATURE	b. NAME (Last, First, Middle Initial)	c. GRADE	d. OFFICIAL POSITION

SECTION II - TERMINATION OF ACCESS TO CLASSIFIED CRYPTOGRAPHIC INFORMATION

I am aware that my authorization for access to classified cryptographic information is being withdrawn. I fully appreciate and understand that the preservation of the security of this information is of vital importance to the welfare and defense of the United States. I certify that I will never divulge any classified cryptographic information I acquired, nor discuss with any person any of the classified cryptographic information to which I have had access, unless and until freed from this obligation by unmistakable notice from proper authority. I have read this agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available to me Title 18, United States Code, Sections 641, 793, 794, 798, and 952; and Title 50, United States Code, Section 783(b).

ACCESS WITHDRAWN THIS _____ DAY OF _____ _____ ,

3. EMPLOYEE - DO NOT EMAIL THIS FORM WITH SSN FILLED IN!!!

a. SIGNATURE	b. NAME (Last, First, Middle Initial)	c. GRADE/RANK/RATING	d. SSN - Pen only!!!

4. ADMINISTERING OFFICIAL

a. SIGNATURE	b. NAME (Last, First, Middle Initial)	c. GRADE	d. OFFICIAL POSITION

SD FORM 572, JUN 2000 PREVIOUS EDITION IS OBSOLETE.

FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE: ANY MISUSE OR UNAUTHORIZED DISCLOSURE MAY RESULT IN BOTH CIVIL AND CRIMINAL PENALTIES.

TITLE 18 - UNITED STATES CODE - CRIMES AND CRIMINAL PROCEDURE

SECTION 641 - PUBLIC MONEY, PROPERTY OR RECORDS

_____ INITIALS

Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof; or

Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted—

Shall be fined under this title or imprisoned not more than ten years, or both, but if the value of such property in the aggregate, combining amounts from all the counts for which the defendant is convicted in a single case, does not exceed the sum of $1,000, he shall be fined under this title or imprisoned not more than one year, or both

The word "value" means face, par, or market value, or cost price, either wholesale or retail, whichever is greater

SECTION 793 - GATHERING, TRANSMITTING OR LOSING DEFENSE INFORMATION

_____ INITIALS

(a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, research laboratory or station or other place connected with the national defense owned or constructed, or in progress of construction by the United States or under the control of the United States, or of any of its officers, departments, or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, stored, or are the subject of research or development, under any contract or agreement with the United States, or any department or agency thereof, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

(b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

(c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter; or

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit, or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or

(f) Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information, relating to the national defense,

(1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or

(2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of its trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer—

Shall be fined under this title or imprisoned not more than ten years, or both

(g) If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy

(h)(1) Any person convicted of a violation of this section shall forfeit to the United States, irrespective of any provision of State law, any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, from any foreign government, or any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, as the result of such violation. For the purposes of this subsection, the term "State" includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States

(2) The court, in imposing sentence on a defendant for a conviction of a violation of this section, shall order that the defendant forfeit to the United States all property described in paragraph (1) of this subsection

(3) The provisions of subsections (b), (c), and (e) through (p) of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853 (b), (c), and (e)–(p)) shall apply to—

(A) property subject to forfeiture under this subsection;

(B) any seizure or disposition of such property; and

(C) any administrative or judicial proceeding in relation to such property, if not inconsistent with this subsection.

(4) Notwithstanding section 524 (c) of title 28, there shall be deposited in the Crime Victims Fund in the Treasury all amounts from the forfeiture of property under this subsection remaining after the payment of expenses for forfeiture and sale authorized by law

SECTION 794 - GATHERING OR DELIVERING DEFENSE INFORMATION TO AID FOREIGN GOVERNMENT

_____ INITIALS

(a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life, except that the sentence of death shall not be imposed unless the jury or, if there is no jury, the court, further finds that the offense resulted in the identification by a foreign power (as defined in section 101(a) of the Foreign Intelligence Surveillance Act of 1978) of an individual acting as an agent of the United States and consequently in the death of that individual, or directly concerned nuclear weaponry, military spacecraft or satellites, early warning systems, or other means of defense or retaliation against large-scale attack; war plans; communications intelligence or cryptographic information; or any other major weapons system or major element of defense strategy.

(b) Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the Armed Forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct, or supposed plans or conduct of any naval or military operations, or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for any term of years or for life.

(c) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

(d) (1) Any person convicted of a violation of this section shall forfeit to the United States irrespective of any provision of State law—

(A) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and

(B) any of the person's property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of, such violation.

For the purposes of this subsection, the term "State" includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States.

(2) The court, in imposing sentence on a defendant for a conviction of a violation of this section, shall order that the defendant forfeit to the United States all property described in paragraph (1) of this subsection.

(3) The provisions of subsections (b), (c), and (e) through (p) of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853 (b), (c), and (e)–(p)) shall apply to—

(A) property subject to forfeiture under this subsection;

(B) any seizure or disposition of such property; and

(C) any administrative or judicial proceeding in relation to such property, if not inconsistent with this subsection.

(4) Notwithstanding section 524 (c) of title 28, there shall be deposited in the Crime Victims Fund in the Treasury all amounts from the forfeiture of property under this subsection remaining after the payment of expenses for forfeiture and sale authorized by law.

SECTION 798 - DISCLOSURE OF CLASSIFIED INFORMATION

_____ INITIALS

(a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information—

(1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or

(2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or

(3) concerning the communication intelligence activities of the United States or any foreign government; or

(4) obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes—

Shall be fined under this title or imprisoned not more than ten years, or both.

(b) As used in subsection (a) of this section—

The term "classified information" means information which, at the time of a violation of this section, is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution. The terms "code," "cipher," and "cryptographic system" include in their meanings, in addition to their usual meanings, any method of secret writing and any mechanical or electrical device or method used for the purpose of disguising or concealing the contents, significance, or meanings of communications.

The term "foreign government" includes in its meaning any person or persons acting or purporting to act for or on behalf of any faction, party, department, agency, bureau, or military force of or within a foreign country, or for or on behalf of any government or any person or persons purporting to act as a government within a foreign country, whether or not such government is recognized by the United States. The term "communication intelligence" means all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients. The term "unauthorized person" means any person who, or agency which, is not authorized to receive information of the categories set forth in subsection (a) of this section, by the President, or by the head of a department or agency of the United States Government which is expressly designated by the President to engage in communication intelligence activities for the United States.

(c) Nothing in this section shall prohibit the furnishing, upon lawful demand, of information to any regularly constituted committee of the Senate or House of Representatives of the United States of America, or joint committee thereof.

(d) (1) Any person convicted of a violation of this section shall forfeit to the United States irrespective of any provision of State law—

(A) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and

(B) any of the person's property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of, such violation.

(2) The court, in imposing sentence on a defendant for a conviction of a violation of this section, shall order that the defendant forfeit to the United States all property described in paragraph (1).

(3) Except as provided in paragraph (4), the provisions of subsections (b), (c), and (e) through (p) of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853 (b), (c), and (e)–(p)), shall apply to—

(A) property subject to forfeiture under this subsection;

(B) any seizure or disposition of such property; and

(C) any administrative or judicial proceeding in relation to such property, if not inconsistent with this subsection.

(4) Notwithstanding section 524 (c) of title 28, there shall be deposited in the Crime Victims Fund established under section 1402 of the Victims of Crime Act of 1984 (42 U.S.C. 10601) all amounts from the forfeiture of property under this subsection remaining after the payment of expenses for forfeiture and sale authorized by law.

(5) As used in this subsection, the term "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

SECTION 952 - DIPLOMATIC CODES AND CORRESPONDENCE	
_____ INITIALS	Whoever, by virtue of his employment by the United States, obtains from another or has or has had custody of or access to, any official diplomatic code or any matter prepared in any such code, or which purports to have been prepared in any such code, and without authorization or competent authority, willfully publishes or furnishes to another any such code or matter, or any matter which was obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States, shall be fined under this title or imprisoned not more than ten years, or both

FINAL ACKNOWLEDGEMENT				
* I HAVE READ THE INFORMATION GIVEN ON THIS FORM AND UNDERSTAND ALL MATERIAL WITHIN. IF I HAD ANY QUESTIONS, THEY WERE ANSWERED TO MY SATISFACTION.				
EMPLOYEE				
SIGNATURE		PRINT		GRADE

DEBRIEFING SECTION				
SECTION 783 (B) - RECEIPT OF, OR ATTEMPT TO RECEIVE, BY FOREIGN AGENT OR MEMBER OF COMMUNIST ORGANIZATION, CLASSIFIED INFORMATION				
It shall be unlawful for any agent or representative of any foreign government knowingly to obtain or receive, or attempt to obtain or receive, directly or indirectly, from any officer or employee of the United States or of any department or agency thereof or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, any information of a kind which shall have been classified by the President (or by the head of any such department, agency, or corporation with the approval of the President) as affecting the security of the United States, unless special authorization for such communication shall first have been obtained from the head of the department, agency, or corporation having custody of or control over such information.				
EMPLOYEE				
SIGNATURE		PRINT		GRADE

SAMPLE LETTER/MEMORANDUM OF APPOINTMENT

FOR OFFICIAL USE ONLY – PRIVACY ACT SENSITIVE: ANY MISUSE OR UNAUTHORIZED DISCLOSURE OF THIS INFORMATION MAY RESULT IN BOTH CRIMINAL AND CIVIL PENALTIES

From: Commanding Officer or Staff CMS Responsibility Officer (SCMSRO)
To: (Rank, Name, DoD EDIPI/MOS)

Subj: APPOINTMENT AS THE KEY MANAGEMENT INFRASTRUCTURE OPERATING ACCOUNT MANAGER/ALTERNATE (KOAM)

Ref: (a) EKMS-1 (Series) Supp-1
(b) DoD 8570.01 (series)
(c) Management Client (MGC) Operational Security Doctrine (OSD)
(d) Enrollment of KMI Managers Doctrine
(e) Registration of KOAs and KMI Users Doctrine
(f) Operational Security Doctrine (OSD) for the Skey6500
(g) Dod 1000.30

1. In accordance with reference (a), you are hereby appointed as… for this command.

2. KOA account number: _____.

3. Date and Location of completion of the KMI formal course of instruction or Date-Time-Group (DTG) of the NCMS waiver approval if not previously competed:

4. Security clearance data: _____.

5. Additional KMI roles, not prohibited by policy held by the appointee.

6. You will familiarize yourself with the references (a) – (g) to ensure compliance in your execution of duties for the roles appointed.

Signature of Commanding Officer or
Staff CMS Responsible Officer

COMSEC ACCOUNT MANAGER TURNOVER CHECKLIST

Item	Conducted by	Witnessed by	Remarks
Pending Receipts	Outgoing Manager	NA	(1) Request an up-to-date Pending Receipts Report from NCMS. (a) For any physical material reflected with a TN date 30 days or longer, **the outgoing manager will report non-receipt to the command which initiated the transfer.** (b) If any electronic key is reflected, the outgoing manager will connect to the X.400 message server, download the material (BETs) in the mailbox and submit the receipts or report of corrupt BET, as applicable within 96 hours in accordance with EKMS-1(series) Article 742. (c) If any BETs cannot be processed and they contained modern key, it **MUST BE REORDERED.** *Tier-1 cannot resupply modern key.*
Change of Manager Inventory	Outgoing Manager	Incoming Manager	Requires 100% sight inventory of all COMSEC material (less embedded COMSEC installed in equipment) including keying material, book-packaged material, equipment, CIKS, etc... * **Ensure KAMs, KAOs, Q-kits and book-packaged material is page checked and such is recorded in the Record of Page check page.** Also ensure all Inventory Reconciliation Status Transaction (IRST) discrepancies are corrected or the required action has been taken **PRIOR TO** assuming the account.
Verify Reserve on Board (ROB) levels	Outgoing Manager	Incoming Manager	Ensure levels are adequate for operational requirements. See the matrix in EKMS-1B Article 620 and report shortages to NCMS and CMIO. Example: If the edition supersedes annually the unit should have a minimum of the current +1; semi-annually the current +2, quarterly the current +2. **Do not have only the currently effective edition of key and no ROB as an emergency supersession will result in a critical circuit outage or possible COMSEC incident.**
Pending Outgoing Transactions	Outgoing Manager	Incoming Manager	Ensure receipts for any material transferred are processed. To verify if any outstanding transactions exist, go to: **Accounting – Reconcile – Hard Copy Receipt or Accounting- Reconcile – Electronic Receipt, as applicable.** Contact the recipient to verify the material was received and request the receipt be returned for processing.
Verify Modern Key holdings	Outgoing Manager	Incoming Manager	**Ensure a minimum of 05 copies of modern key required for each network/enclave are ordered prior to turning over the account.** Go over each supported network/enclave with the incoming manager. If any are closed partitions, ensure Command Authority information is part of the turnover.

Modern Key Expiration Data	Outgoing Manager	Incoming Manager	(1) Review expiration date information for all modern key held **with emphasis on any expiring within 60 days or which is AOR specific, if deploying. For any not ordered above, ensure key orders are submitted.** (2) Verify the use of the NCMS modern key tracking tool. If not in use, download it, populate the data and make use of it. It can be found via SIPR https://uar.cas.navy.mil/secret/navy/39/portal.nsf - **Modern Key Forms – Modern Key Tracker** **** Remember, modern key doesn't just end up in the units X.400 mailbox; it must be ordered****
Update Common Account Data (CAD)	Outgoing Manager	Incoming Manager	Ensure the accounts CAD data is updated to reflect the new COMSEC Account Manager. See EKMS-704 Chapter 7 (Request EKMS Account Modification)
Update User Registration Data (CF 1206)	Outgoing Manager	Incoming Manager	Update the Central Facility User Representative (UR) Ordering Data. Forms and instructions can be found at: https://www.iad.gov/KeySupport/index.cfm
SKL Audit Review Log	Outgoing Manager	Incoming Manager	Verify the log exists for the current year and prior (02) years. If the log does not exist, submit a COMSEC incident report in accordance with EKMS-1B Article 945.E.4.
Combinations /Pins/ Passwords	NA	Incoming Manager	(1) Ensure combinations held by the prior manager(s) are changed and SF-700s are updated and properly stored. (2) Ensure any passwords, including the root password for the LMD or KP pins are changed and recorded on a new SF-700.
Update the USTRANSCOM Form-10	Outgoing Manager	Incoming Manager	Ensure accurate reflection of the new Manager and other account personnel and submit it to the servicing DCS station. EKMS-1(series) Art 405.h.
Update the CMS Form-1	Outgoing Manager	Incoming Manager	(East Coast units only) . EKMS-1(series) Art 405.H; Art 640; Annex H . The form can be copied and edited from the sample in Annex H. The form can be found on the Defense Courier Division (DCD) web page
Access List Updates	NA	Incoming Manager	Ensure the vault access list is updated. EKMS-1(series) Art 505.D.
Letter of Appointment	Outgoing Manager	Incoming Manager	Ensure the Incoming Manager is properly cleared, appointed in writing and executes a SD Form 572. EKMS-1(series) Art. 412, 418, 505, Annex K
KP Changeover	NA	Incoming Manager	Conduct a KP Changeover, label the new NAVREINIT 2s properly, conduct a LMD backup and zeroize the old NAVREINIT 2s (EKMS-704 9-65). Ensure future KP Changeovers occur every 92 days at a minimum. (EKMS-1B
			Art 238.B.2; Art 945.C.8)

KP Rekey	NA	Incoming Manager	(1) Verify there are **no** BETs on the desktop. If so, unwrap them and reconcile for the material. (EKMS-704 Paragraph 10-24, 10-7, 4-48). (2) If any BETs cannot be unwrapped/processed follow the BAD BET procedures in EKMS-1(series) Art. 742.D (3) Conduct the KP Rekey (EKMS-704 9-17), process the Rekey Response and post the new credentials by connecting to the Directory Service and "UPLOAD OWN" CAD.
Status Information	NA	Incoming Manager	Do not carry out destruction or issue material without first verifying the accuracy of status information applied to the material or reflected in LCMS.
General Message Review	Outgoing Manager	Incoming Manager	Verify all COMSEC-related ALCOMs, ALCOMPAC P (PACFLT units) and ALCOMLANT ALFA (LANTFLT units) is held. Start with the most recent recap which is ALCOM, ALCOMPAC P or ALCOMLANT ALFA 001/XX (XX = CY)
Command COMSEC Policy	NA	Incoming Manager	Review the Command, ISIC and TYCOM COMSEC policies.
Transit CIK, FF Vector Set, and MSK	Outgoing Manager	Incoming Manager	Verify there are no previously loaded Transit CIKS, FF Vector Sets or MSKs on the Accountable Item Summary (AIS) : EKMS-1(series) Article 238; 1005.A (Note: You will always get a new Transit CIK when the KP is replaced. The Transit CIK (USKAU B7121) when loaded becomes the 1st sysadmin CIK and must be recorded as destroyed. The MSK when loaded created the REINIT1 and NAVREINIT 2 KSD-64As and also must be recorded as destroyed. The FF Vector Set (USFAU 0000000333), when loaded is used to enable generation and exchanging of credentials to exchange or receive electronic keying material. It is a SEED key and must be recorded as "Filled in End Equipment" not "destroyed" when loaded. It is kept up-to-date through the required annual KP Rekey.
KP Recert	Outgoing Manager	Incoming Manager	Verify the certification date on the accounts KP. If it expires in six months or less or the command will be at-sea when it expires coordinate early replacement with CMIO and NCMS. EKMS-5(series) Article 202
Backups & Archives	Outgoing Manager	Incoming Manager	Verify backup media and archives are on file, labeled and safeguarded at the secret level. A LCMS backup is highly recommended during assumption of duties to ensure an up-to-date tape is available should the LMD fail.

Review the most recent COR Audit report	Outgoing Manager	Incoming Manager	Identify discrepancies noted, if any and what corrective action was taken.
Conduct an account Self-Assessment	Outgoing Manager	Incoming Manager	At a minimum Annex A to EKMS-3C will be used. If time permits, a minimum of (3) LEs should also be assessed using Annex C to EKMS-3 (series).
Training	Outgoing Manager	Incoming Manager	Review the commands long and short-range training schedule and ensure COMSEC training in part of the schedule. EKMS-1(series) Art. 455.F
Spot Checks	Outgoing Manager	Incoming Manager	Review spot checks completed by the CO and the COMSEC Account Manager(s). 16 total are required per year (Art 450/455/1005.A.17). (4) by the CO; (2) of which can be delegated and (1) per month by the COMSEC Account Manager or Alternate(s).
KAMs/KAOs/ Q-kits	Outgoing Manager	Incoming Manager	If excess copies are held, the account has KAMs/KAOs or Q-kits for equipment no longer held, or the account have broken CCI in the account, request disposition instructions for these. EKMS-1(series) Art. 655 and EKMS-5(series) Art 402-403. San Diego ships, mobile units, etc... can use the COMSEC Equipment Exchange Program (CEEP) to have broken CCI replaced through the CRF in San Diego, when assets are available to replace the failed units. See EKMS-5(series) Art. 403
If incidents and/or PDSs are discovered, ensure they are documented and reported, as required. They are likely to be discovered during a visit and/or inspection however, if self-identified and documented/reported, as applicable the unit cannot be cited again.			

I/we certify herein that the actions and areas identified herein have been completed or reviewed and found current and up-to-date.

Outgoing Account Manager		Incoming Account Manager	
Printed Name	Grade	Printed Name	Grade
Signature	Service	Signature	Service

KOAM 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 MGC/AKP system to include, monitor, keyboard, Mouse, scanner, printer, router, UPS, tokens, disaster recovery kit (DRK) and associated cables.

_____b. AKP with AKPREINIT 1 and 2 keys and associated backups.

_____c. STE with key loaded or ready.

_____d. KOAMs Fill Device.

_____e. Security Containers.

_____f. MGC backup disks.

_____g. (2) spare toner cartridges for the printer.

_____h. COMSEC Pubs.

_____i. COMSEC Files to include (Chronological, Correspondence, Directives, General Message File, and Local Custody files).

_____j. Spare batteries as required for T/E Items.

_____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" series lock combo instructions and change key.

_____n. Greenleaf combo locks.

_____o. General office supplies (30 days' worth).

_____p. Operational STE Cards.

_____q. Heavy-duty power down-converters.

_____r. Classification stamps, etc.

_____s. Ammo can for burn destruction.

_____t. 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 KOAM 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 KMI account manager you are relieving in country to determine key requirements in addition to your LEs.

____ 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 the DCS station nearest to your deployed theater of operations.

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

____ 11. If your AKP 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 an AKP rekey within one month of deployment. Post own credentials once rekey has been received from Central Facility.

____ 13. Download and process from the PRSN, all the credentials from accounts you will work with while deployed.

____ 14. Contact the KMI account manager for the unit you will be relieving in country 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 KMI vault/facility/shelter.

_____e. KG-250 Connectivity.

_____f. INMARSAT turnover.

_____g. Projected departure dates for KOAMs 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 "KMI escort plan".

_____a. Will you pallet ride with all KMI equipment?

_____b. Prepare to embark your KMI equipment

_____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. Perform one last database backup prior to packing and label accordingly.

____ 18. Print one copy of AIS and keep in the deployment folder that you keep with you.

____ 19. Ensure that you, the KMI reps from your LE's and possibly your CMR RO's are on the advance party.

____ 20. Backup your MS Outlook .pst files, Internet Explorer favorites, and COMSEC documents to CD-ROM for both SIPR and NIPR accounts.

END OF YEAR PROCEDURES

All COMSEC 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 reference (a) for contents of these files.

Consult Annex M of reference (a) for specific retention periods for COMSEC files.

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

A. Transaction status log: Verify all transactions for the previous 12 months have been reconciled, with no pending transactions.

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 and SD-Form 572.

D. Review all Letters of Agreement.

E. Update USTRANSCOM FORM 10.

F. Update KOAM manager and alternate letters of appointment.

G. Update common account data (CAD).

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

I. Verify date of last archive.

J. Verify date of last AKP rekey and STE/SCIP Products.

K. Verify date of last AKP recertification.

L. Reinitialize SKL and document.

M. Review COMSEC holdings to ensure continuing need for quantity and types of material held; to include Modern Key and TRKEK's.

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

Note: All I MEF accounts will verify to their ISIC by 31 January of each year, via email or naval message, that the above has been completed.

PROCEDURES FOR ROUTINE MODIFICATION OF COMSEC ALLOWANCE

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 account's 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. Requests should be addressed as follows:

TO: NEXT SENIOR FLAG LEVEL COMMAND/ISIC
CC: CMC WASHINGTON DC C4CY
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 OF COMSEC KEYMAT ALLOWANCE CA369XXX

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 YYMM FORMAT FOR TEMPORARY (E.G., 9906 - 9910)
D. INCREASE OR DECREASE, QUANTITY AND JUSTIFICATION
E. PRESENT APPROVED ALLOWANCE
F. DATE MATERIAL NEEDED
G. COMMAND OF ISIC
H. SERVICING DCS STATION
I. POC AND PHONE NUMBER(S)

DEFENSE COURIER SERVICE (DCS) CHANGE OF ADDRESS REQUEST

FROM: KOAM
TO: OLD SERVICING DCS STATION
CC: NEW SERVICING DCS STATION
ISIC
NCMS
CMIO
DIRNSA
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 "dcs_sdni_all@navy.mil" via NIPERNET. EKMS ACCOUNTS ARE REQUIRED TO SUBMIT REQUEST FOR POST DEPLOYMENT AND RE-DEPLOYMENT DCS SUPPORT.

The DCS contact website is http://www.transcom.mil/dcd/

DISPOSITION INSTRUCTIONS

1. Secondary Reparable (SECREP). SECREP, defined as specified items, which are not operationally functional by themselves. SECREPs are components of other associated items.

Note: All GCSS-MC Service Request (SR) numbers must be annotated on the COMSEC Material Report (SF-153) in the remarks column. This annotation will help improve visibility and tracking of COMSEC equipment.

2. Principal End Items (PEI). PEI is one COMSEC item or a combination of COMSEC items configured to meet a defined mission capability. For example, a Support Wide Area Network (SWAN) is a system, which uses a COMSEC device as a component to be mission capable.

Note: Some COMSEC equipment is unique and is assigned as Supply System Responsibility Item (SSRI) to PEI or used in stand-alone configurations (e.g., KG-175D, etc.).

a. After SRs are initiated, ensure that an appropriate level, qualified maintenance technician inspects and attempts the repair of COMSEC equipment. When maintenance technicians find COMSEC equipment un-repairable or uneconomical to repair, a WIR must be submitted to MCLC Albany via the WIR WOLPH system.

CCI TRANSFER/RECEIPT CHECKLIST

____ 1. Ensure you have proper authorization prior to conducting transfer.

____ 2. Confirm correct short title, accounting legend code (ALC) and classification of all items listed on the transfer SF-153 are entered correctly within the MGC database transferred prior to receipt.

____ 3. Have SL-3 extracts or component lists on hand for all controlled cryptographic items (CCI) that contain multiple cryptographic components (maintenance kits).

____ 4. Sight all CCI material and confirm serial numbers and quantities transferred.

____ 5. Verify all hardware modifications using the Mandatory Modification Verification Guide (MMVG), current ALCOM and MARCORSYSCOM messages.

____ 6. Verify software versions on all items, see ALCOM 068/16 and https://infosec.navy.mil for authorized software versions.

____ 7. Ensure devices are equipped with the appropriate number and type of Cryptographic ignition keys (CIK's).

____ 8. Conduct a "joint audit" of all fill devices. The audit trail log for each fill device begins here for the receiving unit. Annotate the first entry of the new audit trail log with "initial audit" and incoming transaction number.

____ 9. Verify field Tamper Recovery CIK's are being transferred for each KG-175/KG-250.

____ 10. Make version / configuration notes on transferred material. Many principal end items (PEI) have CCI material as SL-3 components. Annotate these relationships in a data base to make locating these items in the future easier.

____ 11. Confirm all supporting software and / or support material is being transferred along with PEI. (EXAMPLES INCLUDE: Iridium secure sleeve PINS, KG-250 SSL and key image files)

____ 12. Ensure all classification stickers are removed from CIK tags. CIK's are not to be transferred with unit applied classification markings intact. When zeroized, all associated CIK's are unclassified.

____ 13. If air shipment is involved, remove the primary batteries for the DTD, and ship separately.

____ 14. Ensure all CCI is zeroized.

____ 15. Ensure all supply transactions are completed for each item transferred.

REQUIRED ACCOUNTING AND CONTROL PROCEDURES

1. KMI. KMI is an interoperable collection of systems, facilities, and components developed by the services and agencies of the U.S. Government to automate the planning, ordering, filling, generation, distribution, accountability, storage, usage, destruction and management of electronic key and other types of COMSEC material. The overall KMI architecture consists of four layers or tiers. Each tier is part of a higher tier. For example, a Tier 3 (Local Element), must be assigned to a Tier 2 (KMI Account).

(a) Tier 0. The Central Facility, or Tier 0, consists of the National Security Agency's (NSA) Fort Meade and Finksburg Key Facilities. Tier 0 provides centralized key management services for all forms of COMSEC key.

(b) Tier 1. This layer of KMI serves as the intermediate key generation and distribution center, central offices of record (COR), privilege managers, and registration authorities for COMSEC accounts. Management of the system is a cooperative effort involving the Navy, NSA, Joint Staff, (J6), Army, and Air Force. Two Primary Tier 1 sites (Lackland AFB, San Antonio, TX and Ft. Huachuca, AZ) house the physical servers that are used for accounting and will provide for the generation and distribution of many traditional key types for large nets.

(c) Tier 2. The layer of KMI comprised of the COMSEC Accounts that manage key and other COMSEC material. Tier 2 accounts are equipped with a Client Host/Management Client (MGC) and interfaces with an Advanced Key Processor (AKP). This suite of equipment is referred to as a MGC/AKP. Tier 2 accounts receive electronic key from Tier 0, Tier 1 or other Tier 2 accounts.

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

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 I MEF or other authoritative source (e.g., material's controlling authority and ISIC).

3. General Control. COMSEC material must be handled and safeguarded based on its assigned classification and Accounting Legend Code. COMSEC material is centrally accountable to the NCMS and the command's COMSEC account. Control of COMSEC material is accounted for through a continuous chain of custody receipts using transfer reports, 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). ALC determines how COMSEC material is accounted for within the KMI system. There are five ALC's 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, along with the SL-3 items, equipment must be accounted for on the units Table of Equipment and local Consolidated Memorandum Report (CMR) or Global Combat Support Systems-Marine Corps (GCSS-MC).

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 non-reportable Practice Dangerous to Security.

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.

9. Safeguarding COMSEC Material. 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.

10. 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 COMSEC 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.

11. Access to COMSEC Equipment (LESS CCI). Access to keyed and un-keyed 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. 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 individuals that require access to the COMSEC equipment, but not the keying material, in the performance of their duties, (i.e., vehicle crewman, 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.

12. 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 22 Aug 2011 Committee on National Security Systems Instruction (CNSSI) 4005. 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 I MEF 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 COMSEC Manager or Alternate Manager.

d. The individual signs an SD-572 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.

13. 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 Kaba-Mas X-09 or X-10 with no one person authorized access to both combinations.

14. Storage Requirements. COMSEC material will be stored only in containers and spaces approved for their storage. Unless COMSEC material is under the direct control of authorized persons, keep the containers and spaces locked. Store COMSEC material separately from other classified material in accordance with reference (a).

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

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

(c) An SF-702 form must be maintained for each COMSEC storage container. Completed SF-702's will be retained for 30 days beyond the last date recorded.

(d) Optional 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. Completed SF-701's will be retained for 30 days beyond the last date recorded.

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

15. 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 COMSEC material is stored. A monthly visual check is required to ensure no tampering or compromise of the envelope and this check must be documented and retained.

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

16. 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 command Security Manager for rules, responsibilities, and briefing on courier duties. Transporting CCI to the Repairable Issue Point does not require being assigned as a courier.

17. Physical Security Survey (PSS). Approval to hold classified COMSEC material must be granted in writing by the ISIC. 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 COMSEC accounts within their responsible area with written authorization to hold COMSEC material up to the Highest Classification Indicator (HCI) of the COMSEC account. ISIC's will authorize a facility to hold COMSEC material at a minimum of every 12 months during the COR Audit.

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

18. COMSEC Incident. All COMSEC Incidents will be reported per Chapter nine of reference (a), I MEF G-6 will be cc'd on all message traffic.

19. Destruction. The COMSEC Manager and Alternates are responsible for the complete and prompt destruction of all COMSEC 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 that requires checking 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 calendar 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 Advanced Key Processor.

(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 COMSEC 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 COMSEC 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.

20. 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 against the controlling authorities current effective status messages. 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. All copies of issued or reissued keying material must be destroyed prior to completing system destruction procedures.

21. 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.

22. 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.

23. 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 (DCS) 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.

DEPLOYMENT PLAN

1. 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 COMSEC material in support of the various Operational Plans (OPLANs).

(a) When a unit deploys, the COMSEC 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 COMSEC account is left behind, a COMSEC Manager or Alternate Manager must remain behind to operate the account. Every six digit COMSEC account requires a COMSEC Manager or Alternate Manager at all times.

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

2. MEF 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 Joint COMSEC Management Office (JCMO) for all services in that theater. The JCMO is designed to provide COMSEC support for a Joint Command. 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 I MEF COMSEC 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 COMSEC material to the entire MEF.

3. COMSEC Deployment Examples. When a unit deploys, it will also deploy the COMSEC account unless there is a Regionalized Deployment Plan which is outlined below.

(a) Regionalization Deployment Plan. This plan requires prior planning. One or two COMSEC accounts will be established within a defined geographical area (OCONUS) to support multiple units within that 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, SD-572 Forms and all other required documentation must be completed with the servicing COMSEC account.

(b) Commanding General (CG) 1st MarDiv, CG 1st MLG, and CG 3d MAW are responsible for providing pre-deployment guidance and assistance to subordinate commands with COMSEC account. In addition to this order, ISICs may implement more stringent requirements.

4. MEU Deployments. 30 days prior to deployment, the MEU COMSEC Manager will submit a Modification of Allowance via the I MEF MCMO. The MEU will normally deploy with the current month plus nine months Reserve on Board (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 (8) 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 COMSEC Manager at least 90 days prior to deployment.

(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 COMSEC account. The MEU COMSEC 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 COMSEC 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.