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

I MEFO 2281.1B
G-6 MCMO
28 JUN 2021

I MARINE EXPEDITIONARY FORCE ORDER 2281.1B

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

Subj: COMMUNICATIONS SECURITY STANDING OPERATING PROCEDURES
SHORT TITLE: (COMSEC SOP)

Ref: (a) CMS 1 (Series)
(b) MCO 2281.1 (Series)
(c) MARFORPACO 2230.1 (Series)
(d) CMS 3 (Series)
(e) MCO 5530.14 (Series)
(f) SECNAV M-5510.30
(g) SECNAV M-5510.36

Encl: (1) Communications Security Standing Operating Procedures
(2) I MCMO Controlling Authority Keying Materiel Request
(3) I MCMO Asymmetric Key Request Form

1. Situation. Key management infrastructure (KMI) is the overarching communications security (COMSEC) system providing the capability for generation, distribution, management, and destruction of electronic cryptographic keying materiel (keymat), as well as the keymat and non-keymat related COMSEC items. The different types of COMSEC materiels include, but are not limited to, cryptographic keymat, equipment, documents, firmware, or software that embody or describe cryptographic logic and other items that perform COMSEC functions. The proper handling, accounting, safeguarding, usage, and disposition of COMSEC materiel is vital in protecting information which if compromised, could jeopardize national security and endanger current operations.

2. Cancellation. I MEFO 2281.1A

3. Mission. Supplement the references with I Marine Expeditionary Force (I MEF) specific guidance for the procedures concerning the appropriate handling of COMSEC materiel and the proper management of KMI operating accounts (KOA) within I MEF.

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. For I MEF commands to ensure that all personnel involved in the handling, controlling, safeguarding, storing, issuing, accounting, usage, and destruction of COMSEC materiels familiarize themselves with the contents of this order.

(2) Concept of Operations. In accordance with (IAW) reference (b), 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 (CAM) and ISICs to discuss policy changes, and identify current trends that affect mission accomplishment. Additionally, the MCMO will manage a COMSEC audit program to ensure compliance with references (a) and (d).

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 producing COMSEC materiel systems (CMS) training facility to provide basic entry level certification to newly appointed KMI operating account managers (KOAM).

(2) MSCs shall: Appoint in writing an ISIC to maintain a COMSEC audit program and serve as subject matter expert within the respective MSC.

c. Coordinating Instructions. Submit all recommendations for changes to this order to the I MEF, G-6 MCMO director via the appropriate chain of command.

5. Administration/Logistics. COMSEC account managers subordinate to the I MEF command structure are required to maintain a copy of this order.

6. Command and Signal

a. Command. This order is applicable to all I MEF commands that utilize COMSEC materiel.

b. Signal. This order is effective upon date signed.

K. S. HECKL

TABLE OF CONTENTS

CHAPTER 1

ROLES AND RESPONSIBILITIES

1. General. This chapter outlines the roles and responsibilities within the I MEF command structure, and provides further guidance to national, Department of the Navy (DON), and Marine Corps COMSEC policies.

2. MEF COMSEC Management Office (MCMO)

a. Role. Serve as advisors to the I MEF commanding general and subject matter experts on all I MEF COMSEC related issues.

b. Responsibilities. The MCMO's responsibilities include, but are not limited to, the following:

(1) Oversee all aspects of the I MEF COMSEC program.

(2) Ensure compliance with all COMSEC publications and official guidance.

(3) To serve as the controlling authority/command authority for all I MEF cryptographic keying materiel.

(4) Disseminate all COMSEC correspondence from higher headquarters to MSCs.

(5) Serve subordinate units as the executive agent on all COMSEC matters.

(6) Serve as ISIC for all I MEF Information Group (MIG) COMSEC accounts and for all MSCs within the MEF.

(7) Oversee all COMSEC planning and operations.

(8) Facilitate the collective reporting of requested information to senior commands, as needed.

(9) Develop and maintain a comprehensive, formal COMSEC audit program IAW reference (d) and the guidelines outlined in chapter 3 of this order.

(10) Manage the I MEF commanding general's COMSEC account, which provides COMSEC support to the MEF command element and commands within the MIG, and the 1st Marine Expeditionary Brigade (MEB) account which exists for deployments/contingency operations as needed.

(11) Validate all COMSEC materiel modification of allowance requests, and forward to higher echelons.

(12) Ensure COMSEC policies are followed, to fulfill national, Department of Navy, and the Marine Corps operational requirements.

(13) Track all COMSEC incident reports (CIR) and reportable practice dangerous to security (PDS) messages released by COMSEC accounts under the I MEF command structure.

3. MSC ISIC

a. Role. ISICs are senior COMSEC representatives appointed in writing by MSC commanding general's, and are under the purview of the I MEF MCMO to serve as the senior representative, responsible for administrative oversight of all COMSEC matters for their subordinate commands.

b. Responsibilities. The MSC ISIC responsibilities include, but are not limited to, the following:

(1) Oversee all COMSEC planning and operations of the MSC.

(2) Collect requested information and forward to the MCMO as needed.

(3) Validate all COMSEC materiel modification of allowance requests from subordinate commands, and forward to the MCMO or controlling authority, as appropriate.

(4) Maintain COMSEC audit program for all subordinate COMSEC accounts.

4. Commanding Officers (CO) of Commands with a Six Digit COMSEC Account

a. Role. Provide effective oversight of COMSEC account management with regard to properly safeguarding, accounting for, handling, and the disposition of COMSEC materiel as well as compliance and enforcement of Navy, Marine Corps, and I MEF COMSEC policies.

b. Responsibilities. The CO's responsibilities include, but are not limited to, the following:

(1) Be accountable for all CMS functions and handling procedures within their commands.

(2) Appoint in writing, qualified members of the command as the KOAMs to conduct the administration of routine matters for the command's KOA.

(3) Attend the "CMS for commanding officers" training, offered by the MCMO, no later than three months after assuming command, if available.

(4) Ensure COMSEC materiel storage facilities are properly certified and comply with physical security requirements.

(5) Ensure KOAMs and persons handling COMSEC materiel hold appropriate clearances and are properly trained to handle COMSEC materiel. If the KOAM is a uniformed military member, ensure his/her fitness report has KMI annotated as primary duty. If he/she is a civilian, ensure the employee's position description reflects KMI/COMSEC as a primary duty with pertinent responsibilities clearly delineated therein and in the performance appraisal reporting process.

(6) Conduct unannounced spot checks on the account manager and local elements (LE) utilizing the checklists in reference (d) on a monthly basis. The CO can delegate 10 of the spot checks to the executive officer, but must perform at least two spot checks personally IAW reference (a).

(7) Report all COMSEC incidents per reference (a) and ensure the MCMO is courtesy copied on all reports. Reports shall include annotation of corrective measures to bring the account into compliance as soon as possible.

(8) Become familiar with all relevant orders, directives, and references.

5. Staff CMS Responsibility Officer (SCMSRO). At their discretion, the I MEF Commanding General and MSC commanding generals with a six-digit COMSEC account will appoint a SCMSRO to manage the respective command's COMSEC account. This appointment will be in writing and in accordance with reference (a). Their specific roles and responsibilities with regard to COMSEC are identical to those of a commanding officer.

6. KOAMs and Alternates

a. Role. Serve as advisor to the CO or SCMSRO of the six-digit COMSEC account and subject matter expert on all COMSEC related issues.

b. Responsibilities. In addition to the responsibilities identified in references (a) and (b), I MEF KOAM responsibilities include, but are not limited to, the following:

(1) Become familiar with all COMSEC equipment operational security doctrines.

(2) Utilize enclosures (2) and (3) for all I MEF-specific keymat requests.

(3) Attend all MCMO and/or ISIC sponsored training.

Note: All duties and responsibilities for COMSEC clerks and LEs (issuing and using) are outlined in references (a) and (b).

CHAPTER 2

COMSEC ACCOUNT MANAGEMENT

1. General. In addition to the references, this chapter outlines the policies and procedures to be adhered to by all I MEF personnel in the proper execution of their COMSEC account management duties. Proper account management will prevent most occurrences that have the potential to threaten national security.

2. Appointment/Access. To clearly delineate the duties and responsibility of all COMSEC personnel, in addition to the primary KMI manager, an official appointment/access letter is required for the following positions:

a. Alternate Managers. To ensure a two-person integrity (TPI) capability at all times, COs and SCMSROs are required to appoint at least two alternate COMSEC account managers for a total of three. The appointment of the second alternate manager may be tertiary in nature, but all appointed managers need to be familiar with the inner-workings of the command's COMSEC program so as to fulfill the duties in the event that one of the account managers is not available. This requirement pertains to COMSEC accounts with a highest classification indicator (HCI) of top secret, but is also recommended for all COMSEC accounts regardless of HCI.

b. Local Element Custodians (Issuing and Using). COs or officers-in-charge (OIC) of commands that receive COMSEC support from a six digit-account are hereby required to identify an individual to serve as a primary point of contact for that respective LE. That individual will then be appointed in writing by the account CO/SCMSRO. Prior to their appointment, their security clearance must be verified to be at or above the level of required access. They must also complete a Secretary of Defense Form 572 (SD-572). The importance of officially assigning specific COMSEC responsibilities cannot be overemphasized; therefore, when practical, the appointee should be a non-commissioned officer (NCO) or above. The daily duties may be delegated to that custodian, but the responsibility remains at the OIC/SNCOIC level.

c. COMSEC Users. All personnel who require access to COMSEC materiel in the performance of their daily duties must be identified by their respective OIC/CO, and authorized in writing by the account CO/SCMSRO. Prior to their appointment, their security clearance must be verified to be at or above the level of required access. All authorized users of classified keying materiel must also complete a SD-572. See below note for incidental access.

Note: Incidental access is referred to as direct or indirect contact with COMSEC materiel by an individual without an appropriate security clearance. This access is normally through the performance of their official duties (i.e., supply Marine, vehicle operator, generator mechanic/operator, etc.). To alleviate the need to document unauthorized access to COMSEC materiel by way of a CIR, commanders of six-digit accounts are encouraged to publish an official command policy to provide blanket authorization to access unclassified CCI. This authorization does NOT apply to any CCI that contains classified cryptographic keymat or which permits the extraction of such materiel.

3. Portal Management. The I MEF G-6 MCMO portal page is intended to serve as an electronic source containing pertinent I MEF COMSEC information including but not limited to:

a. COMSEC Library. Contains all documents and publications required by reference (a), Article 715.

b. CIR/PDS Tracking Tool. This tool provides for the tracking of unclassified information with regard to all I MEF CIRs and reportable practices dangerous to security.

c. COMSEC Advisories/ALCOMs. The dissemination of relevant COMSEC information is crucial to the proper management of a COMSEC account. Therefore, the MCMO has a consolidated list of COMSEC advisories and ALCOMs on the portal.

Note: The URL for the I MEF MCMO Non-Secure Internet Protocol Router (NIPR) portal page is: https://eis.usmc.mil/sites/imef/G6/MCMO/default.aspx. The URL for the I MEF MCMO Secure Internet Protocol Router (SIPR) portal page is: https://intelshare.intelink.sgov.gov/sites/imef/G6/MCMO/SitePages/Home.aspx.

4. Emergency Action Plan (EAP). Commands that utilize COMSEC materiel are required to create and maintain an EAP IAW Annex (E) of reference (a). The command's EAP must capture unique scenarios that the command may encounter, and the recovery from such scenarios. The below items must be added to each command's EAP:

a. Emergency Destruction Plan (EDP). In addition to an EAP for natural disasters, all I MEF COMSEC accounts (deployable and garrison) will plan for the protection or destruction of COMSEC materiel in the event of hostile actions (e.g., terrorist attack, rioting, or civil uprising).

b. Disaster Recovery Kit (DRK). All I MEF COMSEC account managers will create and maintain a disaster recovery kit to use for rapid recovery in the event of an emergency. Along with the below listed items, COMSEC account managers must maintain a copy of their Accountable Item Summary (AIS) in the DRK. This copy of the AIS must be updated at least quarterly. More frequent updates may be desirable for commands that have a large number of transactions that involve the movement of COMSEC materiel and equipment:

(1) AKPREINIT 1 ironkey USB drive (x2) (stored in TPI security container)

(2) AKPREINIT 2 ironkey USB drive (x2) (stored in TPI security container)

(3) Backup AKP CIK

(4) Database backup media

(5) SF-700s for all user PINs and passwords

(6) Monthly inventory report / product inventory

(7) KOM 3 USB drive

(8) Ghost image disk

(9) All KAR 1, KAR 2, KAR 3, KAR 4, and archive disks

(10) KG-250 disks

(11) Windows product license key document

(12) KOV-29 tokens

5. Equipment Accountability. Accurate accountability and safeguarding of all controlled cryptographic items (CCI) held by a command is instrumental in proper account management. The following is a list of critical functions in the accountability process:

a. CCI Inventory. Account managers are highly encouraged to perform a complete CCI inventory more frequently than the references mandate. Quarterly inventories are recommended.

b. Dual Accountability. CCI maintained at each I MEF command is required to be accounted for using the COMSEC Materiel Control System (CMCS) and the Global Combat Support System-Marine Corps (GCSS-MC). Each accounting systems is independent with specific requirements and supportive of each other system, therefore, neither system takes precedence over the other. COMSEC account managers are required to establish/maintain a good working relationship with their respective supply sections in order to facilitate an appropriate equipment accountability process.

c. Maintenance Procedures. All equipment maintenance actions taken to retain restore COMSEC equipment to an operational status will be performed by authorized maintenance service personnel IAW applicable technical manuals and instructions.

(1) Recoverable Items Report (WIR). When a piece of CCI is no longer rated by a command's table of equipment (T/E), or maintenance personnel find COMSEC equipment to be non-repairable or uneconomical to repair, a WIR must be submitted to Marine Corps Logistics Command (MCLC) via the GCSS-MC service request. WIR is the only authorized method to dispose of obsolete or inoperable COMSEC equipment.

(2) Software Version Upgrades. Modern cryptographic equipment has an embedded and upgradable software capability. Marine Corps Systems Command (MCSC) is the responsible agent for establishing software baselines and configuration management for modern cryptographic equipment used within the Marine Corps. No software upgrades will take place without prior approval from MCSC. For any software upgrades that have been identified as an operational requirement, but have not yet been approved by MCSC, units are required to seek guidance from MCSC and courtesy copy the MCMO on the email correspondence.

d. Equipment Procurement. COMSEC equipment is only procured or increased by submitting a universal needs statement (UNS) or following the

table of organization and equipment change request (TOECR) process. COMSEC equipment procurement requests must be submitted to Combat Development & Integration (CD&I) and MCSC via the unit's G/S-4 and G/S-6 sections, and must include the communication system's capability requirements.

6. Signature Requirements. The standard form-153 (SF-153) used to document the transfer of physical COMSEC materiel/equipment from one six-digit COMSEC account to another six-digit COMSEC account requires two signatures. The first signature will be either the primary account manager or an alternate manager, and the second will be an authorized witness. The account manager, who initiated the transfer, will not sign as a witness. Any witness that signs in block 16 must have written authorization to access the materiel listed on the document.

7. Modification of Allowance (MOA). IAW reference (a), COMSEC account managers are required to perform an annual review of COMSEC keymat holdings. If it is determined that certain keymat short titles are no longer required, or there are short titles the account needs but does not have, an memorandum of agreement must be submitted. I MEF COMSEC accounts will submit all MOA request via naval message to their ISIC for validation and forwarding to the MCMO. In order to ensure proper routing and processing of keymat MOAs, the following guidance must be adhered to:

a. Requests for keymat controlled by Commander, Pacific Fleet (COMPACFLT) must be minimally addressed to the following plain language addressees (PLAs):

(1) TO: ISIC
(2) Information: CG I MEF G SIX
(3) Information: COMMARFORPAC IE DIV
(4) Information: COMPACFLT Comsec Pearl Harbor Hawaii
(5) Information: NCMS Washington DC
(6) Information: CMIO Norfolk Virginia
(7) Information: DIR TIER1 San Antonio Texas
(8) Information: DIR TIER1 Fort Huachuca Arizona
(9) Requesting command (your own PLA)

b. Requests for keymat controlled by U.S. Indo-Pacific Command, U.S. Central Command, or the Joint COMSEC Management Office (JCMO) must be minimally addressed to the following PLAs:

(1) TO: ISIC
(2) INFO: CG I MEF G SIX
(3) COMMARFORPAC IE DIV
(4) USPACOM J6
(5) NCMS WASHINGTON DC
(6) CMIO NORFOLK VA
(7) DIR TIER1 SAN ANTONIO TX
(8) DIR TIER1 FT HUACHUCA AZ
(9) Controlling Authority (CONAUTH)
(10) REQUESTING COMMAND (your own PLA)

c. Message traffic MOAs addressed to any other controlling authority can be validated directly from the ISIC to the ConAuth with I MEF G-6 as a required "INFO" addressee.

d. Certain keymat short titles are requested, at the ConAuth discretion, by e-mail. KOAMs should contact their ISIC if they are unsure which method to use.

Note: Only add the CG I MEF G SIX to the "INFO" line if it is not in the "TO" line.

CHAPTER 3

COMSEC AUDIT PROGRAM

1. General. The COMSEC audit is a formal process to ensure COMSEC account management is conducted IAW established directives. Other tools include spot-checks, training sessions, and command oversight and involvement. A comprehensive and complete audit program is designed to improve COMSEC procedures and educate the people involved. Feedback to the command is the most important aspect of any audit.

2. Audit Specific Responsibilities

a. I MEF MCMO shall:

(1) Identify, in writing, I MEF COMSEC auditors and forward those auditors' names to Marine Forces Pacific.

(2) Ensure auditors are properly trained and meet the requirements set forth in reference (d), Article 301.

(3) Conduct COMSEC audits of MSC/Es as requested, IAW reference (d), Articles 105 and 201.

(4) Provide a semi-annual COMSEC audit program status report to the COMSEC program manager, Headquarters Marine Corps. This report includes any MEF-wide issues or trends associated with the COMSEC audits conducted during that period.

b. Subordinate Commanders and COs shall:

(1) Assume responsibility for ensuring that COMSEC audits are conducted for I MEF subordinate elements located throughout the I MEF area of responsibility to include Twentynine Palms, California, and Marine Corps Air Station Yuma, Arizona.

(2) Ensure KMI managers are conducting self-assessments at least quarterly to identify and correct any deficiencies.

(3) Ensure that the steps to correct the discrepancies found during the formal audit are promptly implemented and appropriate documentation/reports are forwarded to the ISIC.

3. Audit Procedures

a. COMSEC audits are conducted per reference (d). The KMI account and physical COMSEC space, and at least three LEs shall be audited.

b. Each audit shall be unannounced and preceded by an in-brief with the COMSEC account manager. An in-brief with the CO or the SCMSRO is recommended, but not required. During this in-brief, the command will have the opportunity to address any general or specific issues concerning the audit. The auditor is to provide the CO, and others present at the in-brief, an overview of how the KMI account will be audited, the estimated duration of the audit, and an overview of how the out-brief will be conducted.

c. The audit shall cover all areas of account administration and management, and will follow the checklists as outlined in the reference (d).

d. Other than detailed quarterly self-assessments and regular CO's spot checks, special preparations for audits are neither necessary nor should they be undertaken.

4. Reporting Procedures

a. During the audit, the inspector generates a dialog with the KMI manager and alternates. This dialog is an opportunity for information sharing and direct clarification regarding discrepancies, expectations, and recommendations.

b. Upon completion, the auditor shall out-brief the commanding officer or the SCMSRO as applicable. This brief shall include results and recommendations.

c. Within 10 working days of the completion of the audit, the auditor shall provide a formal audit report. This report details the audited command's grade, deficiencies, areas of concern, and recommendations. The final audit report shall be forwarded to the command via the audited command's ISIC.

d. Audited commands are to correct identified deficiencies and return a report of corrective measures to the respective ISIC within 30 days. In the event of an unsatisfactory grade, a re-audit of the account within 90 days from the date of failure will occur.

e. The audit shall be graded IAW reference (d) based upon the administration of the account and the number and type of discrepancies found during the audit.

f. Discrepancies shall be classified as:

(1) COMSEC incidents

(2) Practice dangerous to security (PDS)

(3) Administrative

g. An "outstanding", "noteworthy", or "satisfactory" grade shall recertify the account to hold and store classified COMSEC materiel.

I MCMO
Controlling Authority (CONAUTH) Keying Material (KEYMAT) Request

AUTHORITY:	*As mandated in the CMS 1 (Series) and CNSSI 4006, the CONAUTH is responsible for evaluating COMSEC incidents and authorizing the issuance and destruction of COMSEC material under their control. Pursuant to standing policy, the creation of this form is hereby used to direct issuance and deletion of KEYMAT under CONAUTH (369950) purview.*
INSTRUCTIONS:	*Use this multi-purpose form to add or delete KEYMAT. Complete all applicable sections and submit* the form to the COMSEC Account's Immediate Superior in Command (ISIC) for endorsement. If there is a need for an increase AND decrease, COMSEC accounts are required to submit two separate requests.

***Email Request to :* IMEFMCMO2@usmc.mil** **Subj of Email: "Key Request CAXXXXXX"**

1. ACCOUNT PROFILE:	***Enter the COMSEC account's profile information, as applicable.***	
Command Name	Account Number	Manager Name
E-mail Address	Telephone Number	Date:

2. KEYMAT SELECTION:	***Select KEYMAT to add or delete***		
USEAD G11015 880091 **(KIV 7M SUITE "A" MEDLEY)** ☐	USEAD M4021 880091 **(KG-175 WPPL/ PPK)** ☐	USEAD M4334 880091 **(KIV 7M MEDLEY)** ☐	USEAD M4454 880091 **(HAIPE/ PRC 117G)** ☐
USKAD 1047 880091 **(VINSON/ ORDERWIRE)** ☑	USKAD 222 880091 **(ANDVT/DAMA)** ☐	☐	☐

3. REQUEST TYPE:	***Select either an increase or decrease in KEYMAT***		
Increase: ☑		Decrease: ☐	

4. IN PLACE DATE:	***Enter the dates of your request or if you wish to be added to permanent profile***	
Date Required: From: To:	Permanent Profile: YES: ☐	NO: ☑

5. FOR KOAM USE:	***Enter remarks to support request, if required.***
KOAM Remarks:	KOAM Digital Signature

6. ISIC ENDORSEMENT:	***The ISIC must endorse the request and forward to CONAUTH***
ISIC Remarks:	ISIC Digital Signature:

7. FOR CONAUTH USE:	***Approval will be forwarded to CIMO for processing. Denied request will be sent back to the originating COMSEC account with justification***
CONAUTH Remarks:	CONAUTH Digital Signature:

I Marine Expeditionary Force (MEF)
COMSEC Management Office (MCMO)
Asymmetric Key Request Form

Requestor Identification		
Requestor's Rank and Name		
E-mail Addresses	NIPR:	@usmc.mil
	SIPR:	@usmc.smil.mil
Phone Numbers	DSN:	
	Commercial:	
Date of Request		
COMSEC Account Name		
COMSEC/KMI ACCOUNT ID		

Material Identification		
Short Title (Partition Code)	USFAU 0000033379	
Device Type (Ex: KG-175, KG-250)		
Key Type	X Operational	Seed
Release To:	X U.S. Use Only	Releasable to Allies
Quantity of keys		
Material Classification (Max = TS)	TOP SECRET	

NETWORK INFORMATION	
Network Name (Ex: GCCS-J or CENTRIX-K	JWICS

Justification

I MCMO ACCOUNT INFORMATION	
DSN: 312-365-5901/6224	CONAUTH / CMDAUTH ID: 369950
COMM: 760-725-5901/6224	NIPR Email: imefmcmo2@usmc.mil

Order completed by: _____ **Order completed date:** _____