



DEPARTMENT OF THE NAVY  
HEADQUARTERS UNITED STATES MARINE CORPS  
3000 MARINE CORPS PENTAGON  
WASHINGTON, DC 20350-3000

MCO 2281.1  
C4  
MAY 29 2008

MARINE CORPS ORDER 2281.1

From: Commandant of the Marine Corps  
To: Distribution List

Subj: ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS) POLICY

Ref: (a) EKMS 1A (NOTAL)  
(b) EKMS 3B (NOTAL)  
(c) SECNAVINST 5510.36A  
(d) SECNAV M-5510.36  
(e) SECNAV M-5210.1  
(f) NAVMC DIR 5210.11E

Reports Required: I. COMSEC Incident Reports (Report Control Symbol EXEMPT), par. 3.b.(1)(e) & par. 4.b.(6)(a)  
II. Report of Inspection (Report Control Symbol EXEMPT), par. 4.b.(5)(b)  
III. Practice Dangerous to Security (PDS) Report (Report Control Symbol EXEMPT), par. 4.b.(6)(c)

1. Situation. The Marine Corps EKMS leadership structure, roles and responsibilities, appointment requirements, and specific topics governing the Marine Corps EKMS program do not exist in any Marine Corps Order. This Order corrects that deficiency and aligns the Marine Corps EKMS Program with national Communications Security (COMSEC) policy and Department of the Navy (DON) EKMS procedures that govern Marine Corps EKMS requirements.

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

3. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. The intent of this Order is to ensure that all commands adhere to proper EKMS management procedures for the protection of COMSEC throughout the Marine Corps. The nature and sensitivity of COMSEC material (equipment, keying material and publications) requires positive accountability and management by the EKMS Manager out to the Local Element. Therefore, it is paramount that all General Officers (GOs), Staff Communications Material Responsible Officers (SCMSROs), Commanding Officers

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

(COs), and Officers in Charge (OICs) exercise prudent leadership (Momentum, Commitment, Teamwork, and Reciprocity) to ensure maximum compliance.

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

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

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

(c) Teamwork (i.e., are the EKMS designees working together). Recognize high-performing Marines and publicize their accomplishments. Publicize the things that one unit does to help another.

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

b. Tasks

(1) General Officer (GO), Commanding Officer (CO), Officer in Charge (OIC). The individual who is ultimately responsible for the proper management and security of COMSEC material held by his/her command. The responsibilities of GOs, COs, and OICs for EKMS are not abrogated upon delegation of management and oversight duties. GOs, COs, and OICs must:

(a) Receive annual Commanding Officer's Briefings.

(b) Ensure compliance with established EKMS policy and procedures.

(c) Appoint qualified individuals in writing as Staff Communications Material System (CMS) Responsibility Officer (SCMSRO), Immediate Superior in Command (ISIC), EKMS Manager, Alternates, and Account Clerk as outlined in reference (a).

(d) Establish a list of personnel authorized access to keying material (keymat).

(e) Ensure COMSEC incident reports (i.e., Initial or Amplifying) are promptly and accurately submitted to appropriate officials, including C4IA. Submit COMSEC incident reports as outlined in reference (a). This

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

(f) Conduct unannounced Spot Checks at least quarterly.

(g) Establish and periodically test the Emergency Action Plan (EAP) or Emergency Destruction Plan (EDP).

(2) Staff CMS Responsibility Officer (SCMSRO). Perform and assume all authorities for routine COMSEC matters of a GO in command status (or any officer occupying the billet of a GO with command status). SCMSROs specific responsibilities are identical to those of a GO, CO, or OIC.

(3) Immediate Superior in Command (ISIC)/EKMS Inspector. Responsible for the administrative oversight of all COMSEC matters for their subordinate commands' EKMS accounts. ISIC responsibilities include:

(a) Validating the operational requirements for EKMS accounts.

(b) Validating command compliance with the minimum physical security requirements for safeguarding COMSEC material.

(c) Determining the required COMSEC material based on command mission and communications capabilities.

(d) Ensuring that physical security inspections are conducted every two years.

(e) Conducting EKMS account inspections.

(4) EKMS Manager. The individual who is responsible to a GO (or SCMSRO), CO or OIC for the proper administration of the command's EKMS account. The EKMS Manager serves as principal advisor to the command on matters concerning the proper handling of COMSEC material, and the administration of required records and reports.

(5) Alternate EKMS Manager. The Alternate EKMS Manager share responsibility equally with the EKMS Manager for the proper management and administration of the command's EKMS account. [Each EKMS Account should make every effort to appoint a minimum of two Alternate EKMS Managers].

(6) Local Element (LE). Separate entities, units or commands (internal or external to the parent EKMS account) that require COMSEC material to perform its mission. LEs receive COMSEC material from the single EKMS account they are registered to (i.e., a parent account). LEs are normally issued material for immediate use in end cryptographic units (ECUs); conversely, some LEs may routinely issue COMSEC material to other LEs. Refer to reference (a) for additional details on LEs.

4. Administration and Logistics. Recommendations concerning the contents of this Order may be forwarded to CMC (C4IA) via the appropriate chain-of-command.

a. Appointment Requirements

(1) SCMSRO

(a) U. S. citizen.

(b) Commissioned Officer or civilian government employee; O-4/GS-12 (YA, YB or YC 02-03) or above; and, senior to the command's EKMS Manager.

(c) Possess a security clearance equal to or higher than the highest classification of COMSEC material held by the account. Appointment can be based on an interim security clearance.

(d) Possess a working understanding of the command's EKMS account and system requirements and responsibilities.

(2) ISIC/Inspector

(a) U. S. citizen.

(b) Possess a security clearance equal to or higher than the highest classification of COMSEC material possessed by inspected accounts.

(c) Successfully complete the EKMS Manager's Course of Instruction (COI), V-4C-0013.

(d) Successfully complete the Navy's EKMS Inspector training seminar; attend one A&A Training Visit and, assist in an actual EKMS Inspection.

(3) EKMS Manager

(a) U. S. citizen.

(b) Commissioned Officer (with a minimum of six months of service), enlisted E-6 (or above), or civilian government employee GS-7 (YA, YB, or YC 02-03) or above with a minimum of six months of government service. The position description of a civilian government employee must specify EKMS Manager duties as either full-time or collateral prior to appointment.

(c) Possess a security clearance equal to or higher than the highest classification of COMSEC material held by the command. Appointment can be based on an interim security clearance.

(d) Successfully complete the EKMS Manager's Course of Instruction (COI), V-4C-0013, prior to appointment.

(4) Alternate Manager. The appointment criterion for an Alternate Manager (Primary and Secondary) is the same as EKMS Manager, with the following exceptions:

(a) Primary Alternate Manager must complete the EKMS COI within 90 days from the initial date of appointment.

(b) Secondary Alternate Manager must complete the EKMS COI within 180 days from the initial date of appointment.

(5) Local Element (LE). Each LE must be a U. S. citizen, military, government employee or contractor. Refer to reference (a) for additional details. LEs are divided in two categories: Issuing and Using.

(a) Issuing LEs are authorized to issue keymat and CCI to other LEs.

(b) Using LEs are authorized to use keymat, CCI, and keymat.

(6) Account Clerk

(a) U. S. citizen.

(b) Possess a security clearance equal to or higher than the highest classification of the COMSEC material being handled. Appointment can be based on an interim security clearance.

(c) Must be capable of executing his/her administrative COMSEC duties.

b. Required Files and Plans. Maintained by the EKMS Manager; periodically spot-checked by CO (or designee)/SCMSRO, officially inspected by an EKMS Inspector, and results reported to NCMS and C4IA. EKMS Managers are required to maintain the following list of files and comply with the retention and remediation procedures described herein:

(1) Chronological File. Per reference (a), the Chronological File will contain copies of COMSEC material receipts, transfers, destruction, possession reports, inventories, summaries, status logs, conversion notices, and Responsibility Acknowledgment Forms in current calendar year file.

(a) Per reference (e), SSIC 2200.1, retain for a minimum of 2 years or when no longer needed for operations, whichever is later, in EKMS inactive file.

(b) Inactive files denote an inactive status of COMSEC files, records, and logs. The inactive files must be stored separately from the current year's files and clearly labeled with the appropriate classification, disposition authority and the authorized date of destruction per reference (f).

(2) Local Custody File. The Local Custody File will contain all effective signed local custody documents reflecting the issuance of COMSEC material to LEs in current calendar year file. Per reference (e), SSIC 2200.1, retain for a minimum of 2 years or when no longer needed for operations, whichever is later, in EKMS inactive file.

(3) Correspondence, Message, and Directives Files

(a) The Correspondence File will contain:

1. EKMS account registration correspondence.
2. Appointment correspondence.
3. COMSEC incident and PDS reports.
4. Correspondence relating to equipment and keying material allowances and authorization to store classified COMSEC material.
5. Advice & Assist (A&A) visits and Inspection

correspondence.

6. List of personnel authorized access to keying material.

7. List of personnel authorized access to the Local Management Device/Key Processor.

(b) The Message File will contain all effective general messages (e.g., ALCOMs, ALCOMLANT ALFAs, ALCOMPACs, etc.) that pertain to account holdings or COMSEC policy and procedures.

(c) The Directives File will contain a copy of each effective directive of the command and higher authority that relates to COMSEC matters (e.g., guidance for LEs, Letters of Agreement (LOA) and waivers of COMSEC policy and procedures).

(d) Emergency Action Plan (EAP)/Emergency Destruction Plan (EDP). Each command, that holds classified COMSEC material (including Controlled Cryptographic Items [CCI]), must prepare and maintain a current, written EAP/EDP for safeguarding such material in the event of an emergency. A major disaster may include fire, tornado, earthquake, bomb threat, or hostile actions (terrorist attack, rioting, or civil disturbance). The EAP/EDP must describe responsibilities and actions to take to safely evacuate or securely destroy the affected COMSEC material. The EKMS Manager is responsible for maintaining the COMSEC material portion of the Command's EAP/EDP.

(4) Storage and Handling. Adhered to and enforced by the EKMS Manager; periodically spot-checked by CO (or designee)/SCMSRO; and, officially inspected by an EKMS Inspector and results reported to NCMS and C4IA.

(a) Storage facilities for COMSEC material must provide the maximum practical protection from pilferage, theft, compromise, damage and deterioration. Storage facilities must be inspected every twenty-four (24) months by a Marine Physical Security Specialist or by a Security Manager for Marine Corps Reserve accounts that are not located aboard Marine Corps installations. A copy of the Physical Security inspection must be submitted to the command ISIC for issuance of a Command Certification. Unless in use or continuously attended by an appropriately cleared person, COMSEC material will be stored separately from other classified material. General Service Administration (GSA) approved safes are the preferred method of storage for COMSEC material.

(b) Handling. Key tape and/or electronic segments will not be removed from its canister or uploaded to an ECU until immediately prior to use or destruction.

(5) Inventories, Inspections and Training. Adhered to by the EKMS Manager and LEs, periodically spot-checked by CO (or designee)/SCMSRO, and officially inspected by an EKMS Inspector and results reported to NCMS and C4IA.

(a) Inventories. Conduct inventories semiannually of all COMSEC material holdings (including publications/manuals and equipment) with Accounting Legend Code (ALC) 1, 2, 4, 6, and 7.

(b) Inspections. Inspect EKMS Accounts every 2 years; more frequent inspections are authorized and encouraged. The EKMS inspector will inspect the command's EKMS account, its administrative records, command involvement during the past two years, and LEs. Discrepancies discovered may be beyond the control or corrective capability of the present EKMS staff and should not adversely reflect upon their performance. Inspections must be unannounced and conducted by a NCMS certified EKMS inspector. All inspections are conducted using questions outlined in reference (b). At the conclusion of the inspection, the EKMS Inspector will provide the inspected command a copy of the completed checklist and the recommended inspection grade. Additionally, the inspector will provide C4IA (i.e., EKMS Program Manager) a copy, via Portable Document Format (PDF) or facsimile, of the official Report of Inspection letter and a list of all findings discovered during the inspection, and corresponding recommendations. This report is exempt from reports control under SECNAV M-5214.1, Part IV, paragraph 7.j. Inspection results are graded as Satisfactory or Unsatisfactory.

1. Satisfactory indicates that the command is following correct DON policies and procedures, even though minor discrepancies may be found.

2. Unsatisfactory indicates that numerous discrepancies were discovered during the inspection and that established policy and procedures are not being followed.

(c) Training. Receive Advise & Assist (A&A) Training visits every 18 months from the Navy's A&A Team. Additionally, the EKMS Manager must conduct training on specific COMSEC issues (i.e., Secure Telephone Equipment, Data Transfer Devices, Simple Key Loaders, EAP, etc.) for LEs at least quarterly. All training must be documented and maintained in the account's Correspondence File.

(6) COMSEC Incidents and Practices Dangerous to Security (PDS). Adhered to by the EKMS Manager and LEs, periodically spot-checked by CO (or designee)/SCMSRO, and officially inspected by an EKMS Inspector and results reported to NCMS and C4IA.

(a) COMSEC Incidents. Incident reporting applies to all COMSEC material, equipment, and publications. Submissions of incident reports are mandatory, and required when cryptographic or physical incidents occur. COMSEC incidents must be promptly reported. The COMSEC Incident report is submitted as outlined in chapter 9 of reference (a). This report is exempt from reports control under SECNAV M-5214.1, Part IV, paragraph 7.d. The EKMS Manager and GO/SCMSRO, CO, or OIC are responsible for ensuring that National Security Agency (NSA) and C4IA are included on each incident (i.e., Initial, Amplifying, Close) report. NSA enters the incident information into its COMSEC Incident Trend Analysis (CITA) database, which provides national trend analysis reports to departments and agencies to promote COMSEC awareness and remedial action. C4IA enters the information into its local database for trend analysis and remedial action.

(b) Practice Dangerous to Security (PDS). If allowed to perpetuate, a PDS has the potential to jeopardize the security of COMSEC material. All PDSs must be immediately brought to the attention of the EKMS Manager and corrected accordingly. Each EKMS account will conduct annual PDS familiarization training. The familiarization training must include

information outlined chapter 10 of reference (a). Training must be documented and maintained in the EKMS Account's Correspondence File.

(c) Reporting. Each EKMS account will submit PDS reports using the format as outlined in chapter 10 of reference (a). This report is exempt from reports control under SECNAV M-5214.1, Part IV, paragraph 7.k. PDS are divided in two categories: Reportable and Non-reportable. EKMS Account Managers must ensure that each reportable PDS include C4IA as an information addressee on all Defense Message System (DMS) messages.

(7) Marine Corps Specific COMSEC Issues

(a) Equipment Repair Order (ERO)/Equipment Repair Order Shopping List (EROSL). The ERO (NAVMC Form 10245)/EROSL (NAVMC Form 10925) or Float Process is an alternate custody documentation process used in lieu of the COMSEC Material Report (SF-153), by operational or exercising LEs whose parent EKMS Account is not in the same geographical location to provide equipment exchange support. The use of the Float Process (ERO/EROSL) is a temporary measure and does not replace EKMS accounting procedures. The Float Process can be used to document the exchange of CCIs (i.e., equipment) from LEs to Maintenance Battalions (and vice versa). During the Float Process all pertinent accounting data (i.e., short title, serial number, ALC) must be captured. Close coordination between the EKMS Manager of the Maintenance Battalion and the EKMS Manager supporting the LE must be initiated prior to executing the Float Process. The Float Process is authorized only when CCI is in the maintenance cycle (i.e., preventive maintenance or equipment requiring repair).

(b) Incidental Operator. Individuals who operate military vehicles, members of vehicle convoys, Marines who serve as guards, etc., that do not possess the appropriate security clearance for access to keyed COMSEC equipment or crypto-systems. The acquisition and fielding of COMSEC equipment (with embedded cryptographic key) requires Incidental Operators to have access to classified crypto-systems to support missions and exercises. Commanding Officers are authorized to use Incidental Operators in tactical environments, contingent on the following guidelines:

1. Under no circumstances will uncleared (i.e., a person without a security clearance) individuals handle classified keying material or fill devices with classified key fills.

2. All COMSEC material shall be issued on a COMSEC Material Report form (SF-153) to appropriately cleared personnel. Incidental operators shall not be issued keying material or CCI directly to load into cryptographic equipment. The actual loading of keymat into cryptographic equipment is the responsibility of the Manager or LE.

3. The Incidental Operator's official duties includes: Operator of equipment or team member, Tank/Amphibious Assault Vehicles (AAV) convoy/crewmember, guard, Contact Team Member or Forward Observer).

4. The system or network, which the radio is operating, must be a tactical/security radio network.

5. The individual is appropriately indoctrinated in the handling and safeguarding of COMSEC material, and an Acknowledgement of Responsibility form is signed. This guideline may be waived during emergency



combat situations. The Acknowledgement of Responsibility form must state the following:

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

(c) EKMS Inspector Assignment/Certification. Assignment and certification of EKMS Inspectors will occur only after the candidate has successfully completed the prerequisites outlined in reference (b). The A&A team that provided training to the EKMS Inspector candidate will submit a memorandum to NCMS indicating that the candidate successfully completed all required training. NCMS will prepare and forward the Inspector candidate's memorandum to C4IA for endorsement. Upon positive endorsement, NCMS will forward a Letter of Certification recommending assignment as an EKMS Inspector to the candidate's command.

1. In order for an EKMS Inspector to retain a valid certification, the inspector must meet the following requirements:

a. Attend the EKMS Inspector Training Seminar every 36 months while assigned as an EKMS Inspector.

b. Personnel re-assigned as an EKMS Inspector that have been out of the program for a period exceeding 12 months (with all remaining requirements still valid) must re-attend the EKMS Inspector Training Seminar.

c. Additional training, as directed.

2. Upon completion of a subsequent EKMS Inspector Training Seminar, NCMS will forward a Letter of Recommendation for continued assignment as an EKMS Inspector to the Inspector's command.

(d) Realignment of EKMS Accounts. EKMS Accounts will require realignment (i.e., renaming, relocation or disestablishment) when operationally relevant. A request and justification must be submitted by the CO/EKMS Account Manager to the EKMS Chain of Command for approval. After submitting the request and justification, the following procedures will occur (Each procedure must be followed to ensure that appropriate oversight is given to all aspects of the realignment process):

1. The MARFORs/Senior ISICs will thoroughly review the realignment request (i.e., inventory requirements, keying material and equipment disposition, etc.), and forward their recommendation to C4IA for approval.

2. Once the request is approved, C4IA will forward it to the EKMS Account, MARFORs, and NCMS (for updates to databases) via Defense Message System (DMS) message. If the request is disapproved, C4IA will inform the requestor via the chain of command of the decision and rationale for disapproval.

(e) Inspector Instructor/Site Commander as SCMSROs. Commanding Officers/Officers in Charge (OIC) of Reserve units, with active EKMS Accounts, are authorized to designate (in writing) Inspector Instructor/Site

Commander as SCMSRO. Designating a SCMSRO does not relieve reserve commanding officers of their account responsibilities. The CO/OIC shall remain fully engaged in their EKMS Account's transactions during drill weekends and active duty periods.

5. Command and Signal

a. Command. This Order is applicable to the Marine Corps Total Force. The EKMS leadership structure and functional roles are established as follows:

(1) Director for Command, Control, Communications, and Computers (C4). The requirements, administration, and resources sponsor for Marine Corps EKMS accounts.

(2) C4 Information Assurance (IA) Division. Responsible for exercising overall authority of Marine Corps' EKMS matters; promulgation of Marine Corps policy regarding management of EKMS accounts; and, responsible for working with Naval Communications Security Material System (NCMS) and Marine Corps Systems Command to ensure that accounts have the necessary resources to effectively operate.

(3) Marine Forces (MARFOR) Commands. Marine Forces Command (MARFORCOM), Marine Forces Pacific (MARFORPAC), and Marine Forces Reserve (MARFORRES) are responsible for validating COMSEC holdings, providing guidance and oversight to subordinate EKMS accounts, maintaining positive custody, control and administration of COMSEC material in EKMS accounts, and serving as Immediate Superior in Command (ISIC) for respective Marine Expeditionary Forces (MEF).

(4) MEF COMSEC Management Office (MCMO): Responsible for validating COMSEC holdings, providing guidance and oversight of subordinate EKMS accounts; maintaining positive custody, control and administration of COMSEC material in cache accounts for their respective MEFs; and, maintaining Marine Corps EKMS training centers. Serve as ISIC for Major Subordinate Commands (MSCs) and Major Subordinate Elements (MSEs) of respective MEFs.

(5) Installations/Bases/Stations/Units. Responsible for maintaining positive custody, control and administration of COMSEC material in EKMS account including Local Elements (LEs).

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



G. J. ALLEN  
Director, Command, Control,  
Communications and Computers

DISTRIBUTION: PCN 10202851800