UNITED STATES MARINE CORPS
MARINE CORPS AIR STATION YUMA
BOX 99100
YUMA, ARIZONA 85369-9100

IN REPLY REFER TO
2280
EKMS
13 Jun 13

STATION ORDER 2280.2

From: Commanding Officer
To: Distribution List

Subj: ELECTRONIC KEY MANAGEMENT SYSTEM STANDARD OPERATING PROCEDURES

Ref: (a) EKMS Series
(b) SECNAV M5510.36

Encl: (1) MCAS Yuma Local Elements (LEs)
(2) Definitions

1. Purpose. To publish Standing Operating Procedures, in accordance with the references, for the safeguarding, control, distribution, and handling of Electronic Key Management System (EKMS) material within this command.

2. Cancellation. StaO 2280.1

3. Background. EKMS provides for the security of highly sensitive classified communications material and related devices. Positive accountability for all Communications Security (COMSEC) material will be maintained from the time of receipt until destruction or transfer is affected. All personnel involved with COMSEC material must be aware of the safeguards required while handling COMSEC material to ensure appropriate security is maintained. We must prevent the loss of control and/or compromise of material. All personnel having access to electronic or hard copy keying material shall be familiar with the contents of this order.

4. Action. All personnel authorized access to COMSEC equipment or keying material distributed through the MCAS Yuma primary EKMS account will comply with the provision of this order. When confronted by situations not specifically covered by this order, the basic principles of physical security and proper accounting coupled with sound judgment and common sense shall be exercised.

5. Responsibilities

a. Commanding Officer. The Commanding Officer (CO), Marine Corps Air Station (MCAS) Yuma is ultimately responsible for proper management and security of all COMSEC material held by MCAS Yuma and for enforcing compliance with established policy and procedures.

b. EKMS Manager. The EKMS manager is responsible for performing COMSEC duties associated with receipt, issue, safeguarding, accounting and disposition of COMSEC material assigned to the EKMS account. The EKMS

Manager will be appointed in writing by the CO, MCAS Yuma as prescribed by reference (a). The EKMS manager will provide written guidance to LEs in accordance with reference (a).

c. Alternate EKMS Manager(s). A Primary Alternate EKMS manager will be appointed in writing by the CO, MCAS Yuma in accordance with reference (a). The Primary alternate will act in place of the EKMS Manager during his/her absence. Additionally, at least one additional alternate manager will be appointed in writing. Alternate manager(s) must be actively involved in daily operation of the account. The alternate manager may not administer the account for more than 60 days. If the EKMS manager is absent for more than 60 days, a new EKMS manager or LE Manager must be appointed.

d. LE (LE). An LE is defined as any properly cleared and designated individual who accepts local custody responsibility for the use of COMSEC material. The LE will be properly instructed in handling, security, accounting and disposition of COMSEC material. Before receiving COMSEC material, the LE will sign a COMSEC Responsibility Acknowledgement Form and Local Custody Receipt per enclosure (1). Immediately notify the EKMS Manager if an increase is required of any COMSEC material.

e. EKMS Witness. An EKMS Witness is any United States government employee (military or civilian) who assist EKMS personnel in the proper execution of routine task related to the handling and safeguarding of COMSEC material. The individual must be given access to COMSEC material in writing by the CO, MCAS Yuma and be familiar with applicable procedures contained in this order, the references and any subsequent command issued guidance. A witness is equally responsible as the other signatory for the accuracy of the information listed and the validity of the report or record used to document the transaction being witnessed.

6. Procedures

a. Obtaining COMSEC Material Support. Requests for COMSEC support from commands other than MCAS Yuma must be in accordance with the reference (a), and a Letter of Agreement (LOA) must be signed between the requesting command and CO MCAS Yuma prior to support.

b. Local Custody. Local custody is the acceptance of responsibility for proper handling, safeguarding, accounting and disposition of COMSEC material issued by the EKMS Manager. Every person to whom COMSEC material is issued must complete a COMSEC Responsibility Acknowledgement Form. The local custody file must contain all effective, signed, local custody documents reflecting the issue of COMSEC material. This file contains the only documentation of COMSEC material issued locally and access must be controlled appropriately. The local custody file must contain a signed SF-153 for each item of the COMSEC material charged to the individual to which COMSEC material has been issued. LE Custodians must maintain physical custody over their local custody documents.

c. Issuance of COMSEC Material. All equipment, publications, keying material and call sign/frequency booklets issued to LE's will be signed for on an SF-153. COMSEC keying material in hard copy form marked "CRYPTO" will not be issued any earlier than one month prior to the effective period of the material. When receipting for COMSEC material, all LE's will adhere to the following procedures:

(1) Be designated and authorized to sign for COMSEC material.

(2) Present a Department of Defense Identification Card.

(3) When receiving electronic key transferred in Data Transfer Device (DTD), acknowledge transfer of this key by signing local custody documents.

(4) Properly safeguard and continuously account for the DTD by serial number and its associated Crypto Ignition Key's (CIK) until the entire classified key is destroyed).

d. Returning COMSEC Material. Once the COMSEC material is no longer required, the LE Custodian will return the material to the MCAS Yuma EKMS Manager. An SF 153, signed by the managers, will be provided to the LE as proof of return.

e. Storage. Unless COMSEC material is under the direct control of persons authorized access, containers and spaces shall be kept locked. COMSEC material must be stored according to effective status categories (e.g., Superseded, Effective, Reserve on Board) and by classification (e.g., Secret, Confidential). COMSEC material shall be stored only in containers and spaces approved for such storage. Storage space approval is granted in the form of a Physical Security Evaluation (PSE) conducted by the Provost Marshal's Office (PMO). Physical Security Evaluations are performed every two years or as required. It is the responsibility of LE's needing a PSE to contact the Physical Security Chief at PMO. Storage requirements are addressed in the references. Specific physical requirements are addressed in the references. Specific physical and procedural security requirements for storage are contained in reference b. COMSEC material will be stored separately from other classified material.

(1) Only properly cleared and authorized individuals will have knowledge of and access to the combinations of security containers containing COMSEC material. To provide for emergency access, the lock combinations for all security containers must be maintained in a container other than the container where COMSEC material is stored. Combinations to COMSEC material security containers must be protected as follows:

(a) Each combination must be recorded and individually wrapped in aluminum foil and protectively packaged in a separate SF 700 envelope.

(b) Laminate each envelope in plastic or seal plastic tape.

(c) The names and addresses of the individuals authorized access to the combinations must be recorded on the front of the envelope. The EKMS/ LE Manager or alternates must inspect the envelopes monthly to ensure they have not been tampered with. A log will be kept of this monthly check. A statement will be placed on the monthly check log whenever a combination is changed

f. Sealing of COMSEC Material. The sealing or resealing of COMSEC keying material will be done in accordance with reference (a).

g. Reproduction. Reproduction of COMSEC material is defined as the complete reproduction of an entire code, authenticator, call sign, publication or key list regardless of the reproduction method. Material coded by an arrangement of holes (key tape) is not reproducible. Any LEE needing to reproduce COMSEC material must first coordinate with the EKMS Manager. Only the CO, MCAS Yuma can authorize the reproduction of COMSEC material. All reproduced COMSEC material will be accounted for locally.

h. Damaged, Worn or Manipulated Publications and Keying Material. Such publications and material will be returned to the EKMS Manager for replacement.

i. Turn in of Controlled Cryptographic Items (CCI). All equipment, whether damaged or malfunctioning, will be turned into the EKMS Manager for replacement.

j. Modification to COMSEC Equipment. LE/users with EKMS equipment requiring modification will return the equipment to the EKMS Manager, who will in turn issue the LE a modified piece of equipment if available.

k. Inventories

(1) The EKMS Manager will issue LEs custodians an inventory and require them to conduct inventories on the following occasions:

(a) Semi Annually

(b) Change of Command

(c) Change of Custodian

(d) As Required

(2) The following procedures pertain to the conduct of all inventories:

(a) All individuals conducting the inventory must sight the short title, edition and accounting number of the COMSEC material held.

(b) Perform page checks on all publications and keying material.

(c) When completing the inventory report, LE custodians will note any corrections to the report using black ink. Entries will be lined out as appropriate and the YYMMDD will be inserted in the remarks column. Inventory discrepancies will be noted and brought to the attention of the EKMS Manager for correction. The last page of the inventory will be signed by two individuals inventorying the material. Do not add material to the last page of the inventory.

(d) LEs will return the signed inventory to the EKMS Manager.

l. Spot Checks. The CO, MCAS Yuma will perform a quarterly spot check on the EKMS account as prescribed in reference (a). LEs shall perform a monthly spot check on those personnel within their command performing EKMS duties utilizing reference (a). These spot checks shall be done by an officer or Staff NCO.

m. Two Person Integrity (TPI). Handling requires that at least two persons, who are authorized access to COMSEC keying material, be in constant view of each other and the COMSEC material requiring TPI whenever that material is accessed and handled. Each individual must be capable of detecting incorrect or unauthorized security procedures with respect to the task being performed. For specific details on what type of material requires TPI refer to reference (a).

n. Destruction. Attention to detail is paramount when destroying COMSEC material. Failure to follow proper procedures is one of the principle causes of incidents and practices dangerous to security. Keying material marked or designated CRYPTO is the most sensitive item of COMSEC material. Immediate, complete and proper destruction of superseded keying material is of the highest importance. Destruction of regularly superseded EKMS material will be done in accordance with the following procedures:

(1) Both persons destroying COMSEC material are equally responsible for the timely and proper destruction of the material and the accuracy of the destruction report.

(2) Prior to destroying any COMSEC material, verify, validate, and sight each item of material to be destroyed and ensure that it is, in fact, superseded and/or authorized for destruction.

(3) One individual will read the short title and accounting data of the material to be destroyed, while the witness will verify the destruction document against what the first individual reads. The two individuals will then swap duties and repeat the process again.

(4) LEs must ensure that complete physical destruction has been accomplished within the timeframes contained in reference (a).

(5) LEs will contact the EKMS account manager for guidance in all cases involving the irregular or emergency supersession of EKMS material.

(6) CCI equipment will not be destroyed and the LE level.

(7) The following methods may be used to destroy paper COMSEC material:

(a) Burning

(b) Crosscut shredding (Must be an NSA approved device for key tape and paper material)

(c) Pulping (Reduce to no larger than 5 mm) key tape will not be pulped

(d) Pulverizing

(8) The completed and signed SF-153 destruction report will be returned to the EKMS account manager within three working days after the material is destroyed.

(9) The CMS 25 will be retained by the LE as proof of proper-segmented destruction.

(10) COMSEC material may not be destroyed prior to its authorized destruction date. Additionally, EKMS material must be destroyed in the allowable time frame. Failure to destroy COMSEC material within the allowable time frame is a locally reportable Practice Dangerous to Security and will be handled in accordance with the guidelines set forth in paragraph 7 of this order. If unsure of the destruction date of the material, contact the EKMS Account Manager to determine destruction periods of the material.

7. COMSEC Material Incidents / Practices Dangerous To Security (PDS)

a. Purpose of Reporting. The purpose of reporting COMSEC material incidents is to provide controlling authorities with necessary information to evaluate incidents, to take action to minimize or eliminate the potential for compromise of classified information and to take steps to reduce the possibility of reoccurrence. All personnel who use COMSEC material must be trained in the use and safeguarding of that material in order to recognize COMSEC material incidents as they occur. All personnel who handle or use COMSEC material shall report an incident/PDS immediately upon discovery.

b. Responsibility for Reporting. Reports of any incident must be made irrespective of the judgment of the EKMS Manager or his/her supervisor as to whether or not an incident or possible incident occurred. Disciplinary action will normally not be taken against individuals for reporting a COMSEC incident unless the incident occurred as the result of willful or gross neglect by those individuals.

c. Reporting Criteria. Incidents will normally be reported by the unit that detected the incident. The unit that detected the incident may or may not be the unit that caused the incident. Any actual or suspected loss or compromise will be reported immediately to the MCAS Yuma EKMS Manager. The EKMS Manager will then notify the CO, MCAS Yuma. If in doubt as to whether an incident has occurred, contact the EKMS Manager for a determination as to whether a formal report is required.

d. PDS. PDS's are practices which have the potential to jeopardize the security of EKMS material if allowed to perpetuate. All LEs shall conduct PDS familiarization training that will, at a minimum, include a review and discussion of PDS'S. All training will be documented locally per the guidelines set forth in command directives. Documentation of this training will be forwarded to the EKMS Manager.

8. Emergency Action Plan (EAP). Planning will focus on natural disasters and will be directed toward maintaining security control over the material until order is restored. Planning for hostile action will concentrate on the safe evacuation or secure destruction of the EKMS material. EAPs will be reviewed semiannually for completeness and practicability. EAPs will be of sufficient detail so that personnel totally unfamiliar with COMSEC material and procedures would be capable of correctly executing the plan. Emergency action drills will be conducted at least annually to ensure that personnel are familiar with the plan associated equipment. The drills will also be used to evaluate the anticipated effectiveness of the plan and prescribed equipment and should be the basis for improvements in the planning and equipment use. Records of drills will be maintained for two years.

9. Visitors Log. The EKMS Manager will maintain visitors log to be used whenever personnel not on the authorized access list to the EKMS secure room/vault are granted access to the storage area. The log will contain the individual's name, unit, signature, date, time in/out, reason for visit and the signature of the EKMS Manager or Alternate Manager authorizing the visit.

10. Required EKMS Files. The EKMS Manager will establish and maintain the following files:

a. Chronological File

(1) All accounting reports will be retained for two years

(2) The Chronological File will be used to maintain the following:

(a) Accountable Item Summary retains until updated summary is generated.

(b) COMSEC material accounting reports that document:

1. Transfer

2. Destruction

3. Inventories

(c) Responsibility Acknowledgment Forms

b. Correspondence and Message File. The Correspondence and Message File will be used to document the following:

(1) EKMS Manager(s) and clerk appointment correspondence; retain for two years after the individuals have been relieved of their duties.

(2) COMSEC incident and PDS reports.

(3) Correspondence relating to the command allowance and authorization to store classified material.

(4) EKMS assist visit reports and inspection correspondence.

c. General Message File. Must contain all effective general messages, (e.g. ALCOM's, ALCOMPACP's) that pertain to account holdings or EKMS policy and procedures.

d. Directives File. Must contain a copy of effective directive of the command and higher authority that relates to COMSEC matters (e.g. guidance for LE's, (LOA), and waivers of COMSEC policy and procedures).

e. Local Custody File. Must contain all effective and signed local custody documents reflecting the issue of COMSEC material. The local custody file will contain a signed document for each item of EKMS material charged to the LE. Local custody documents will be retained for 90 days after supersession.

f. EKMS files. Records and logs will be handled and stored in accordance with their overall classification. These are not COMSEC materials.

11. Training. Training is an important part of COMSEC handling and will be conducted on a monthly basis by the EKMS Manager for the LEs. LE Custodians will conduct training for all other personnel within their command. Once completed, a roster of those that received the training will be maintained in

the local custody file. The EKMS Manager will assist the LEs with their training requirements when requested.

12. Secure Terminal Equipment (STE) Responsibilities. The STE is the new generation of secure voice and data equipment designed for use on advanced digital communications networks, such as Integrated Services Digital Network (ISDN). The STE consists of a host terminal and a removable security core. The host terminal provides the application hardware and software. The security core is the KOV-21 cryptographic card that provides all the security services.

a. Observation of the Terminal Display. When two terminals communicate in the secure mode, each terminal automatically displays the authentication (identification) information of the distant terminal. Classified information must not be transmitted during any of the following conditions:

(1) The validity of the authentication information in the display is questionable (even when voice recognition is possible). Authentication information should be representative of the organization in which the distant terminal is located.

(2) The display indicates that the distant terminal's key expired.

(3) The display indicates that the distant terminal contains compromised key. This occurrence also constitutes a reportable COMSEC incident.

(4) The display fails.

b. Control of Terminal Access. Access to keyed terminals must be restricted to authorized users only. When operationally required, authorized persons may permit others not normally authorized to use the keyed terminal in the secure mode under the following conditions:

(1) The call must be placed by the authorized user.

(2) After reaching the called party the caller must identify the party whose behalf the call is being made and indicate their level of clearance.

c. Use of the Hands-Free feature. Use of the hands-free feature of the STE during the conduct of classified conversations is approved provided:

(1) All participants in the conversation have a valid security clearance and an established "need to know" basis for disclosure of the classified information being discussed.

(2) Procedural controls are established to preclude unauthorized personnel from overhearing the conversation. Typically, these controls

consist of ensuring that unauthorized personnel are not within the "earshot" of the conversation.

d. Control of STE and associated KOV-21

(1) While the STE is not CCI, it will be accounted for in the same manner as CCI by the EKMS Manager.

(2) An SF-153 will be used to properly document the local custody issue of STE terminals.

e. Unkeyed (with the KOV-21 removed), The STE must be protected as a high dollar value sensitive government property. The STE must be protected in a manner of sufficient to prevent loss and tampering. A keyed terminal (with the KOV-21 inserted) assumes the highest classification of the inserted card, and must be protected and stored in accordance with established classified material handling procedures. A STE with a KOV-21 inserted may not be left unattended to prevent possible unauthorized use. However, the STE may be left unattended when a KOV-21 is not inserted.

f. Electronic Re-Keying. The terminal user is responsible for performing electronic re-keying as required annually. Note that the terminal user can view the key expiration date on the terminal's display. This indicates the month and year that the user should call the Central Facility for a scheduled re-key.

ROBERT C KUCKUK