UNITED STATES MARINE CORPS
MARINE CORPS LOGISTICS BASE
814 RADFORD BOULEVARD
ALBANY, GEORGIA 31704-1128

BO 2010.1H
112
21 Sep 98

BASE ORDER 2010.1H

From: Commanding General
To: Distribution List

Subj: INTERNAL DISTRIBUTION AND CONTROL PROCEDURES FOR COMMUNICATIONS SECURITY MATERIAL SYSTEM (CMS)

Ref: (a) CMS-21
(b) OPNAVINST 5510.1H
(c) BO P5500.3G

Encl: (1) CMS Responsibility Acknowledgment Form
(2) Emergency Action Plan for CMS Materials
(3) Handling of Crypto Ignition Keys (CIK)

1. Purpose. To set up procedures for the distribution and control of CMS distributed material.

2. Cancellation. BO 2010.1G.

3. Summary of Revision. This Order has been updated to include STU/CIK accountability and to reflect current procedures.

4. Background. The CMS details the security of certain highly sensitive classified material/equipment. Because of the nature and sensitivity of CMS distributed material, positive accountability for the material is required from the time of entry into the system until destroyed or transferred from the CMS. Detailed instructions for issue, accounting, handling, safeguarding, destroying and disposing of CMS material are outlined in the references.

5. Responsibilities

a. EKMS Manager

(1) Per reference (a), the Commanding General will appoint a EKMS Manager, in writing, by official command correspondence. The EKMS Manager is responsible to the Commanding General for the proper administration for the Command's CMS account. The manager also serves as the principle advisor to the Commanding General on matters for the proper handling of Communications Security (COMSEC)

material and required records and reports. The duties and responsibilities of the Electronic Key Management System (EKMS) Manager are outlined in reference (a).

(2) The EKMS Manager reports to the Staff CMS Responsibility Officer (SCMSRO) concerning routine, day-to-day CMS account matters. The EKMS Manager will make immediate notification to the SCMSRO on matters of grave importance or emergency situations affecting on-line operational equipment or procedures. The EKMS Manager will report action taken, and any other matters considered of equal importance.

b. Alternate EKMS Manager. The Commanding General will also appoint a primary alternate manager. The alternate will be appointed, in writing, by official command correspondence. The alternate manager will help the EKMS Manager with CMS duties. The duties and responsibilities of the alternate EKMS Manager is outlined in reference (a).

c. SCMSRO. The Commanding General will appoint a senior staff officer as SCMSRO, in writing, by official command correspondence. The appointed Responsibility Officer shall be granted authority to sign routine reports and CMS correspondence as "Staff CMS Responsibility Officer" and to perform routine command CMS responsibilities. The duties and responsibilities of the Command CMS Responsibility Officer are outlined in reference (a).

d. EKMS Middle Management. The EKMS Manager is not exclusively responsible for the management and security of CMS distributed material. Management and security of CMS distributed material are inherent responsibilities at all levels of command. Proper evaluation of the CMS administrative procedures can only be made by those officials in the chain of command who understand CMS requirements. Officials senior to the EKMS Manager in the operational chain of command will familiarize themselves with the management and security requirements of CMS distributed material.

e. Local Element. A properly cleared and authorized individual using CMS distributed material under specific guidance in the proper performance of duty is a local element. A local element is accountable to the EKMS Account Manager for the CMS distribution material in use.

f. CMS Witnesses. Any member of the command who has proper clearance and training from the custodian may witness destruction, enter amendments, conduct page checks, or witness the inventory of CMS distributed material. The CMS witness shall be familiar with the applicable portions of this Order. The CMS witness who signs any related report shares equal responsibility with the originator for the report's accuracy. A CMS witness must be authorized, in writing, access to keying material.

g. Two Person Integrity. Two person integrity means simply that from the time COMSEC keying material is received by the EKMS account command until it is issued to a user, two authorized people must always be physically present whenever the keying material is not in secure storage. Two person integrity is needed at the local element at all times when hard copy keying material is being handled and during destruction.

6. Procedures

a. Storage Requirements

(1) All TPI keying material will be stored in such a manner that a single person, including the EKMS Manager, cannot obtain access. Storage vaults, safes, or approved containers shall have the necessary security protection, normally by using two approved combination locks. No single person shall be authorized access to TPI CMS materials and access to the combination of both locks.

(2) When feasible, CMS material will be stored separate from other classified material.

(3) All keying material will be stored in a separate safe within the EKMS Manager vault until issued to the local element. Once issued to the local element these same guidelines apply.

b. Access. Only those persons who have a "need to know" and possess the proper security clearance shall be granted access to CMS distributed material. Also, each local element must complete a copy of enclosure (1), the CMS Responsibility Acknowledgment Form, certifying that they have read and thoroughly understand the applicable provisions of references (a) and (b), and this Order. Gaining access to keying material requires the continuous presence of two authorized persons, both of whom will remain with the keying material until all necessary transactions are completed and the vault/safe/container is properly secured.

c. Transfer of Material. All transactions for the receipt or return of CMS distributed material between the EKMS Manager and a local element will be effected via a Standard Form 153, COMSEC Material Report.

d. Transport of COMSEC Material. The Defense Courier Service (DCS) is the authorized means for transporting COMSEC keying material to this Command. The EKMS Manager and alternate are the only personnel authorized to receive from or deliver material to the DCS.

7. Issuing CMS Material

a. When CMS material is issued to local elements, the person authorized to sign for the material is responsible for ensuring that all personnel who have access to the material are thoroughly instructed in the proper handling of CMS material. The person actually using the material is responsible for the proper security, control, accountability, and disposition of all CMS material they handle. COMSEC material held by approved local elements, on local custody, who are permanently leaving the command, and those who are departing TAD in excess of 30 days will be locally transferred to a new approved element or returned to the parent EKMS Manager. Guidelines contained in reference (a) will be adhered to at all times.

b. At the time the CMS monthly issue is made to the local element by the EKMS Manager, there will be a minimum of four custodians present. They are the EKMS Manager, at least one alternate, the local element, and at least one other properly cleared person. This will ensure that the two person integrity requirement is not violated.

c. Watch-to-Watch Inventory

(1) While on duty, each watch supervisor is responsible for the COMSEC material listed on the watch-to-watch inventory. Each watch supervisor will inventory all pertinent COMSEC material. The inventory will be conducted by any appropriately cleared and authorized individual designated by the oncoming watch supervisor. In the case of COMSEC material requiring two person integrity, the inventory must be signed by the two individuals who completed the inventory.

(2) Any discrepancy discovered during the watch-to-watch inventory must be reported immediately to the watch supervisor and the EKMS Manager.

(3) Article 835 of reference (a) lists additional information about watch station COMSEC material management. The watch supervisor will ensure that personnel designated to conduct watch-to-watch inventories are thoroughly familiar with this article.

(4) The watch-to-watch inventory will be retained by the local element for 30 days beyond the last recorded inventory date on the sheet.

8. COMSEC Material Insecurities. Any actual or suspected loss or compromise of CMS distributed material will be reported immediately to the EKMS Manager. The EKMS Manager will notify the SCMSRO and the Base Security Manager and take necessary action, including the prompt preparation of required reports per the references.

9. Changes, Corrections, and Modifications. The EKMS Manager will ensure all changes and corrections to CMS publications and modifications to CMS distributed equipment are entered promptly and correctly. The EKMS Manager will take the following course of action when changes or corrections are received at this Command.

a. Determine the effective date of the change or correction. Consideration will be given to the extent of the change and the required action of cognizant personnel to figure how far in advance of the effective date a change would be entered. Changes that are effective on receipt shall be entered within 5 working days after receipt.

b. The EKMS Manager will ensure that all corrections and changes are entered and is encouraged to use those personnel utilizing the publication or equipment to make the change.

c. The person entering the change/correction/modification will record the information on the Record of Changes/Corrections/Modifications page in the front of the publication. Reference (a) will be used as a guide for entering changes and corrections to COMSEC material.

d. The person making the change/correction/modification will return all residue from the change to the EKMS Manager for destruction.

e. After the EKMS Manager has verified the change has been entered correctly, the running inventory will be annotated within the remarks section to reflect the change.

f. The EKMS Manager will ensure all personnel entering amendments and corrections are provided written guidance on the proper procedures to be used in accordance with article 860 of reference (a). Personnel making amendments and corrections will be furnished a copy of the check list for entering amendments to publications contained in figures 8-2 and 8-3 of reference (a).

10. Removal of CMS Material. Under no circumstances will CMS distributed material be removed from this Command by anyone other than the EKMS Manager or alternates.

11. Destruction of CMS Material. The EKMS Manager is responsible for the complete destruction of all CMS material when authorized for destruction by reference (a) or general message. Destruction will be accomplished per reference (a).

a. Routine Destruction. Destruction of all routine paper CMS material will be accomplished by approved destruction methods per reference (a).

(1) Superseded CMS material, including unused keying material, will be returned to the EKMS Manager for destruction.

(2) Used keying material, including codes and authenticators will be destroyed by the element as soon as practicable after it has served its purpose, but in any case, within 72 hours. SF-153, Destruction Report, will be utilized by local elements to record destruction.

b. Emergency Action Plan. The EKMS Manager is responsible for ensuring that the Emergency Action Plan, enclosure (2), is current and available to designated personnel authorized to receipt for COMSEC material. Personnel designated as local elements are responsible for ensuring that a copy of this plan is posted in all areas where COMSEC material is stored. The EKMS Manager will review the Emergency Action Plan as required for corrections and feasibility.

12. Security Telephone Unit (STU)

a. General. STU COMSEC material is used to protect sensitive and classified U. S. Government voice and data transmissions. STU COMSEC materials consist of a specially designed telephone called the Secure Telephone Unit terminals which is capable of being loaded with COMSEC keying material. These terminals may be used as an ordinary telephone, connectable through the public telephone network to other STU terminals. In the secure mode, each STU terminal displays authentication information of the distant STU terminal. This is possible because of the keying material each terminal contains. The unit's secure mode is activated and deactivated using a device called a cryto-ignition key (CIK). The STU CIK's was developed for use with the STU Secure Voice Phone. It enables an individual to talk in a secure voice mode or transmit data without fear of wire tapping.

b. STU Custodian Responsibilities and Duties. The custodian is responsible to the Commanding General for the proper management of the Command's STU COMSEC material and normally is the Commanding General's primary advisor concerning the physical security and handling of STU materials charged to the Command. In this capacity, the Custodian must also:

(1) Provide the Commanding General and other interested officers with information about new or revised STU policies and procedures and their impact on the Command.

(2) Acquire, monitor, and maintain the Command's STU COMSEC material holdings.

(3) Maintain proper storage and adequate physical security of the STU COMSEC materials held by the account.

(4) Keep the alternate custodian informed of the status of the account so that the alternate is fully capable of assuming full custodian responsibilities at all times.

(5) Provide to the user personnel written guidance or appropriate extracts from the CMS 21 concerning the handling, accountability, and disposition of the STU terminal, keying material, and associated master and user CIK's. Emphasis must be placed on material accountability, security, and the material compromises. Training must also include proper STU key loading.

(6) Issue STU terminals and associated CIK's and STU COMSEC keying material on local custody to properly cleared and authorized users. Ensure that all users are issued a CIK, execute enclosure (3).

(7) Perform STU key loading and CIK creation, as required.

(8) Ensure that all STU terminals are electronically rekeyed as required by the CMS 21.

(9) Maintain records and file as required by the CMS 21.

(10) Ensure the proper local inventory of the STU COMSEC keying material, terminals, and associated CIK's held by users.

(11) Ensure that all amendments to the CMS 21 are entered properly and correctly.

(12) Comply with authorized methods and procedures for destruction of STU COMSEC keying material.

(13) Ensure prompt and accurate preparation, signature, and submission of account correspondence, message, and accounting reports.

(14) Conduct required account inventories of STU COMSEC material in accordance with this Order.

(15) Report immediately to the Commanding General any known or suspected insecure practice of STU COMSEC incident in accordance with the CMS 21. Initiate action to ensure that required reports are submitted and obtain replacement material, if required.

(16) Maintain proper physical security measures when transporting or shipping STU COMSEC material.

13. Managing STU Terminals

a. Responsibility

(1) EKMS Manager is responsible for all STU terminals charged to the account and for managing them in accordance with the CMS 21.

(2) Any movement of STU terminals between elements of the same account must be coordinated with and conducted by the EKMS Manager.

(3) Installation, repair, and maintenance of STU terminals are the responsibility of the account Command.

b. Accountability. STU terminals are accountable to the Director, Communications Security Material System Central Offices of Record by the serial number from receipt to destruction. STU terminals are categorized as controlled cryptographic items.

14. Managing STU Keying Material

a. Responsibility. Only the custodian or users having local custody signature responsibility may retain STU keying material.

b. Accountability. STU operational and seed keying material is AL 1 and is accountable to the Key Management System (KMS) by number from receipt by an account until destructive. AL 1 STU keying materials remain in the KMS central account office database and is charged to the receiving account until the receiving custodian transfers or destroys the material and reports the transfer or destruction to the KMS in the appropriate manner.

15. STU Users. Whether the users have or have not signed personally for STU materials which they are authorized to use, STU users are responsible for the proper security and accountability of the material in conjunction with the CMS 21.

16. Handling of CIK's

a. Procedures

(1) Authorization. In order to use a CIK you must have access to the STU phone and have a CIK issued by the EKMS Manager. The CIK will be issued as an unclassified, confidential, secret, or top secret key depending on the clearance of the user and the location of the phone to which it is designated. The CIK is a personal key issued to the user for their use only and may not be loaned to another.

(2) How to Use the CIK. The CIK can be inserted and turned at any time before or during the conversation in a non-secure mode. After first making your non-secure call, inform the other party you wish to go to a secure mode. At that time you must have your CIK in your phone and the party on the other end must have their CIK inserted and turned to the right. One of the two parties must initiate the secure mode by pressing the secure voice button. The secure voice light will blink for about 15 seconds then will stay on. At that time you will be able to carry on your conversation in a secure mode. Watch the screen during this process, it will display the other parties personal identification as it does your on the other end. It will also display the security level you can talk on. If you have a secret CIK and the other party has a confidential CIK, it will display a secure level of confidential; in other words, it displays the lower of the two clearances. That is as high a level as you should talk. If the secure mode fails, press the non-secure button and start the procedure over again. If it fails a third time contact the EKMS Manager at extension 5208. To disengage the secure mode, press the non-secure voice button or hang up. Both methods will disengage the CIK.

(3) Security. The CIK is the responsibility of the CIK holder. Never leave the CIK unattended in or near the STU phone to which it is assigned. At the end of the day, user CIK's may be kept in personnel possession of the authorized users who signed for them or secured in the office in a security container approved for the classification level of the terminal keys.

(4) Annually, your CIK must be electronically rekeyed. You have the ability to display the key expiration date on the terminal display by following a vendor-specified procedure. You must call KMS at 1-800-635-6301 to rekey your CIK. KMS will provide instructions to electronically rekey your CIK.

b. Lost or Stolen CIK's. Should your CIK be lost or stolen, notify the Base Security Manager at extension 5210 or the EKMS Manager at extension 5208. The EKMS Manager will delete the CIK from the terminal and issue another providing he has a master CIK for that phone. If there is not a master CIK it must be reordered, which takes approximately 2 weeks.

c. Ordering CIK. Send a memo to the EKMS Manager requesting a CIK with the following information:

LAST NAME:
INITIALS:
RANK or GS RATING:
SECURITY CLEARANCE:
OFFICE TITLE: (not to exceed 20 characters)

OFFICE CODE:
EXT:

The security clearance, office title, and office code will be what is displayed on the screen on the phone one ordered.

d. If job titles, transfers, termination of employment, or clearance lowered or withdrawn below the level of CIK access, the CIK must be turned into either the EKMS Manager or the Base Security Manager.

17. Training

a. All personnel having access to COMSEC material will be provided annual COMSEC training by the individual who has responsibility for the material that an individual has access to. The EKMS Manager will provide training to designated persons who are authorized to receipt for COMSEC material from the CMS vault. The individual who receipts for COMSEC material and in turn issues it to someone else, is responsible for that person's training. The EKMS Manager will assist in providing training when requested. This training will be documented by the users and a roster of those receiving the training will be provided to the EKMS Manager.

b. All personnel who handle CMS material must be trained on Practices Dangerous to Security (PDS). At a minimum, training will include a review and discussion of Chapter 14 of reference (a).

c. All training/briefings conducted as required by this Order and reference (a) will be documented by maintaining attendance rosters. A copy of all attendance rosters will be provided to the EKMS Manager for retention.

18. Applicability. This Order is not applicable to the Blount Island Command.

L. P. Cole

L. P. COLE
Chief of Staff

DISTRIBUTION: CMS Custodian (25)
Base Inspector (1)
G4 (2)
Maintenance Center (1)
Fleet Support Center (2)
Base Files (2)

CMS RESPONSIBILITY ACKNOWLEDGMENT FORM

From: (Rank/Rate, Full Name, SSN, and Command of CMS User)
To: EKMS Manager, MCLB, Albany, GA

Subj: CMS RESPONSIBILITY ACKNOWLEDGMENT

Ref: (a) CMS-21
(b) BO 2010.1H

1. I hereby acknowledge that I have read and understand reference (a).

2. I assume full responsibility for the proper handling, storage, inventory, accounting and disposition of the COMSEC material held in my custody and/or used by me.

3. I have received a copy of reference (a) from the EKMS Manager. If at any time I am in doubt as to the proper handling of COMSEC material that I am responsible for, I will immediately contact the EKMS Manager and request advice.

4. Before extended departure from the command (i.e., permanent transfer, or leave/TAD in excess of 30 days) I will report to the EKMS Manager and be relieved of responsibility for all COMSEC material that I am signed for.

Signature:
Date:

ENCLOSURE (1)

EMERGENCY ACTION PLAN FOR CMS MATERIAL

1. Concept

a. The ultimate reason for all security measures is to prevent unauthorized access to classified and cryptographic information. The possibility of unauthorized access is increased during times of emergency. Life safety of personnel is paramount and security considerations secondary.

b. This plan contains instructions and information about protecting classified cryptographic information and material in the event of imminent emergency. At no time will any one individual be permitted lone access to keying material during emergency action procedures.

2. Discussion

a. There are two types of emergencies which can arise. The first is natural disasters, and includes such things as fire, flood, tornado, etc. The second is hostile action and includes enemy attack, mob action or civil uprising. At this Command our concern is with natural disasters, civil mob and terrorism. Since these actions would not normally bring an attempt by hostile forces to capture cryptographic material, planning and actions must be directed to maintaining control over the material until the emergency has passed, or perhaps to moving the most sensitive material to a safer place.

b. When an emergency occurs, there are three options available for the protection of classified material.

(1) Securing. This option includes securing all publications and materials stored in safes, and ensuring the safes are locked. Time permitting, simply lock up all material in an approved security container, vault, or strong room. This is the most convenient method of ensuring unauthorized access.

(2) Removing. Classified material should be removed in a systematic manner and every effort should be made to prevent viewing of material by unauthorized persons. The removal of material should not interfere with fire fighting or subject personnel to unnecessary danger. Every effort must be made to remove classified material from the workplace and have it secured in one of the following locations:

(a) CMS vault, Building 3500.

ENCLOSURE (2)

(b) CMCC vault, Building 3500.

(c) LRCC vault, Building 3700.

(d) Maintenance Center vault, Building 2200

(3) Destroying. Not considered under this action plan since we are only considering natural disasters.

c. Emergency Situation Involving a Fire. In the event of a fire in the workplace, the individual detecting the fire will sound the alarm and immediately notify the Fire Department at extension 5911.

(1) Attempts to suppress the fire should be initially undertaken by assigned workplace personnel. Supervisors should use their discretion in determining what effort should be placed on suppressing the fire.

(2) Individuals who are working with COMSEC material should make sure that all material is returned to proper storage or to one of the locations identified in paragraph 2b(2) of this enclosure, prior to evacuating the area.

(3) In the event that fire fighters or other persons not authorized access to secure areas must enter a secure area, the person having responsibility for the COMSEC material (the person who signed for it) will, if at all possible, accompany them and take action to prevent disclosure. This action could be total removal of material; securing it out of sight, or simply covering it up.

(4) STU telephones will be afforded the same protection as any other item of office equipment during an emergency. If at all possible, CIK's will remain with the individual who has signed or it and locked in an authorized storage container. CIK's should never be left in the STU instrument unattended.

(5) Once the emergency has passed, the individual who is responsible for the material (the person who signed for the material) will complete an assessment of the area to determine the possibility of unauthorized exposure of classified material. The report of this assessment will be provided to the EKMS Manager, in writing, within 12 hours after the emergency has passed.

(6) Within 24 hours after the emergency has passed, a post emergency inventory will be completed and results reported to the EKMS Manager/Staff CMS Responsibility Officer (SCMSRO).

(7) Upon receipt of the post emergency inventory, the EKMS Manager/SCMSRO will review the report and ensure that any losses or unauthorized exposures are reported per CMS-21.

d. Emergency Situations Involving Civil/Mob Actions and Terrorism. In the event of a threat of civil/mob actions or terrorism affecting MCLB Albany, Georgia, the local element will immediately secure all CMS material. If CMS keying material is used by the local element no attempt should be made to key equipment until the emergency has passed.

(1) Individuals who are working with COMSEC material should make sure that all material is returned to proper storage or to one of the locations identified in paragraph 2b(2) of this enclosure in the event of an emergency.

(2) STU telephones and unclassified CCI will be afforded the same protections as any other item of office equipment during the emergency.

(3) The Command will hold only the minimum amount of COMSEC material at any given time.

(4) The Staff CMS Responsible Officer or EKMS Manager will direct all emergency destruction of classified COMSEC material. If the decision is made to destroy material BO 5510.5 will be adhered to.

3. All EKMS personnel and personnel within their chain of command will be briefed on the provisions of this plan as part of the training required by paragraph 12 of this Order.

HANDLING OF CRYPTIC IGNITION KEYS (CIK)

From: STU Users
To: EKMS Manager

Subj: HANDLING OF CRYPTIC IGNITION KEYS (CIK)

1. I assume full responsibility for the proper handling and storage of the STU COMSEC material held in my custody. If at any time I am in doubt as to proper handling of the STU COMSEC material I am responsible for, I will immediately contact the EKMS Manager and request advice.

2. Before departing on extended leave, TAD, and upon detachment, I will check out with the EKMS Manager.

SIGNATURE:

DATE:

ENCLOSURE (3)