



## UNITED STATES MARINE CORPS

HEADQUARTERS MARINE CORPS AIR STATION MIRAMAR  
PO BOX 452000  
SAN DIEGO CA 92145-2000

StaO 2601.1

G-6

**22** AUG 2000

### STATION ORDER 2601.1

From: Commanding General  
To: Distribution List

Subj: COMMAND POLICY FOR HANDLING, ACCOUNTING AND CONTROLLING  
COMMUNICATION SECURITY MATERIAL SYSTEM (CMS) MATERIAL

Ref: (a) CMS 21 (NOTAL)  
(b) SECNAVINST 5510.30A  
(c) SECNAVINST 5510.36

Encl: (1) Sample "CMS Responsibility Acknowledgement"

1. Purpose. To ensure the proper distribution, control, security accountability, handling and destruction of all Communication Security (COMSEC) Material under the jurisdiction of Marine Corps Air Station (MCAS) Miramar, CMS Account Number 169126.

2. Background. CMS provides for the security of highly sensitive classified communications materials and related devices. Two-person integrity (TPI) is the security measure taken to prevent single-person access to COMSEC keying material and cryptographic maintenance manuals. Positive accountability for the material will be maintained from the time of its receipt at this command until its destruction or transfer is reported. Detailed instructions for the issuing, accounting, handling, safeguarding and destruction/disposal will be written and promulgated by the CMS Manager within this command. Instructions promulgated by local account will be submitted to the CMS for approval. Maximum interest, cooperation and involvement by all personnel responsible for the safeguarding of CMS distributed material within this command is essential.

### 3. Responsibilities

a. Staff CMS Responsible Officer. An officer, designated by a flag or general officer, who has direct and personal responsibility for command COMSEC material management.

b. CMS Custodian. Per reference (a), the Commanding General will designate a CMS custodian in writing, at the recommendation of the Assistant Chief of Staff (AC/S), G-6. The CMS custodian is responsible to the Commanding General for the proper administration of the command's CMS account. The custodian also serves as the

StaO 2601.1  
22 AUG 2000

principle advisor to the Commanding General on matters concerning the proper handling of COMSEC material and required records and reports. The duties and responsibilities of the CMS custodian are outlined in reference (a).

c. Alternate CMS Manager. The Commanding General will designate three alternate CMS custodians in writing at the recommendation of the AC/S, G-6. The alternate custodians assist the CMS custodian with CMS duties. The duties and responsibilities of the CMS alternate custodians are outlined in reference (a). All CMS alternate custodians must be fully capable of assuming the custodian's duties, and to be available to assist the custodian in the performance of all CMS duties.

d. CMS Middle Management. The CMS custodian 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 CMS administrative procedures can only be made by those officers in the chain of command who understand CMS requirements. Therefore, it is necessary that officers senior to the CMS custodian in the operational chain of command (i.e. executive officer, communications officer and cryptographic security officer) familiarize themselves with the management and security requirements of CMS-distributed material. In matters concerning suspected physical compromise, loss, unauthorized destruction or finding of CMS material, the CMS custodian will report directly to the Staff CMS Responsible Officer; access to this officer shall not be inhibited (Article 440 subparagraph C of reference (a) is germane).

e. Local Account. An organization that requires COMSEC material and functions essentially as subaccount of a numbered account. Local account will comply with the security, control and internal accountability procedures set forth in this instruction. When it is determined by the Staff CMS Responsible Officer and CMS Custodian that a need exists for a section, activity, detachment or component to assume a local account status, they will be designated as such.

f. CMS Users. An individual designated in writing by the Commanding General or Staff CMS Responsible Officer who, regardless of whether or not they have personally signed for COMSEC material, requires COMSEC material to accomplish an assigned duty and has obtained the material from a CMS Custodian. CMS users are accountable to the local account officers in charge (OIC's) from whom the material is received, in the handling, security,

**22 AUG 2000**

accounting and disposition of COMSEC material. Before COMSEC material can be issued, the CMS custodian will ensure that all CMS users execute a CMS Responsibility Acknowledgement Form as shown in the enclosure.

g. CMS Witness. Only custodians, alternates and CMS users (military or civilian) may be CMS witnesses.

#### 4. Procedures

a. Access. Only those individuals who have a "need-to-know" and possess the appropriate security clearance will be granted access to CMS material. TPI will be applied to classified keying material marked CRYPTO as outlined in reference (a). In addition, each CMS user must complete a copy of enclosure (1), certifying that they have read and thoroughly understand the applicable provisions of the references and this Order.

b. Transfer of Material. All transactions concerning the receipt or return of CMS material between the CMS Manager, local account or user will be effected using a Standard Form 153 COMSEC Material report, CMS 17 Computer Custody Card (Hardware), or locally prepared custody form. Local custody records will be retained for 90 days after the material listed is destroyed or transferred from the command. All transfers by local account/users to units outside the command must be through the CMS Custodian.

#### c. Storage

(1) Storage containers (i.e., vaults, strongrooms, safes) used for CMS distributed material will provide the maximum protection against unauthorized access, material damage or deterioration. Unless COMSEC material is under direct control of persons authorized access to it, the containers and spaces shall be kept locked at all times. COMSEC material shall be stored separately from other material (e.g., in separate containers or in separate drawers). Storage containers for COMSEC material outside the CMS custodians' vault/strongroom, safe, will be approved by the CMS account custodian and will meet the requirement of reference (a). Keying material storage requirements are more stringent than for nonkeying material and will meet requirements of chapter 5, paragraph 515 of reference (a).

(2) Combinations to containers used to store CMS distributed material shall be changed only by individuals with the appropriate security clearance who have been formally granted

StaO 2601.1  
22 AUG 2000

access to CMS material (i.e., custodians/alternates/users). Combinations will be changed per chapter 5, paragraph 505 of reference (a) as follows:

(a) Whenever an individual having knowledge of the combination is transferred from the command or no longer requires access to perform duties.

(b) Whenever the combination becomes known, or is suspected to have become known to an unauthorized person.

(c) Every 2 years. The 24-month period will run from any combination change executed for any reason.

(d) When placed in use after procurement.

(e) When taken out of service.

(3) Notice on Container. The following information shall be maintained for each security container or vault used to store classified material as per chapter 5, paragraph 505B of reference (a).

(a) The date the combination was last changed.

(b) The names of individuals who know the combination and who are to be notified should the container be found open.

(c) Brief instructions for action to be taken if the container is found open (e.g., post a guard; notify duty officer; notify individuals who know the combination; do not touch container or its contents). Containers used to store classified material are to be marked with only a number or symbol for identification purposes. There will be nothing on the outside of a container that indicates its contents or the classification of the contents.

(4) Access to Combinations. Access/knowledge to combinations to the custodian's vault, strongroom and safe(s) used for storage of reserve on board (ROB) COMSEC keying material will be limited to the custodian and alternates only. Knowledge of combinations to safes containing CMS material held by local account will be limited to the local users. A record of combinations shall be wrapped in aluminum foil, placed in a Standard Form 700 envelope, stamped with appropriate classification and sealed on both sides with plastic sheeting for filing in a secure, centrally

located safe accessible to the Command Duty Officer (CDO), Security Manger, Classified Material Control Center (CMCC), OIC or Security Specialist. Laminate each combination in a plastic as outlined in reference (b). All CMS keying material in the custodian storage/local account/user storage will be maintained under two-person integrity. At no time will one person have knowledge of both combinations required for access to the custodian's/local user storage.

5. Reproduction. CMS Material will be reproduced by the CMS custodian only, per chapter 8, paragraph 850 of reference (a).

6. Damaged, Worn or Mutilated Publications. Such publications will be returned to the CMS custodian for replacement.

7. Amendments, Changes and Corrections. Amendments, changes and corrections to CMS distributed material will be entered per chapter 8, paragraph 8 of reference (a), and as directed by the CMS custodian. When entering amendments, changes and corrections, the check-off guide in chapter 8, figure 8-2, Check-Off List, of reference (a) must be used. Both individuals, one of which will be either the local account custodian or alternate, will complete the guide. Once completed, the check-off guide and entry verification form will be returned to the account custodian. Destruction of residue/superseded/revised document will be destroyed and reported by the account custodian when and as directed.

8. Local Destruction of COMSEC Keying Material. TPI must always be used per reference (a).

a. Superseded Keying Material. Superseded CMS keying material which has been unsealed must be page checked prior to local account custodian/alternates conducting destruction.

b. Destruction Procedures for Superseded Portions of Segments. Local account users may destroy/witness destruction of superseded keying material. Superseded keying material will be destroyed not later than 12 hours after supersession. Under no circumstances will superseded keying material exist when a watch/duty section is relieved. Destruction of CMS keying material will be per the following procedures:

(1) The material being destroyed will be separated from all other material. Material for retention will be removed from the general area in which destruction will take place.

StaO 2601.1  
**22 AUG 2000**

(2) The material being destroyed will be arranged in the same order as it appears on the corresponding local destruction record (e.g., CMS 25).

(3) The short titles and accounting data of the material to be destroyed will be verified by the two authorized individuals in the following manner:

(a) The individual responsible for conducting the destruction will read the short titles, edition suffix or material system (MATSYM) (if any), register numbers and/or accounting numbers, to the witness who verifies the information against corresponding destruction record. To preclude inadvertent or unauthorized destruction of material, care will be taken to ensure that pages or cards are not stuck together.

(b) In turn, the witness will read the short titles, edition suffix or MATSYM (if any), register numbers and/or accounting numbers, and segment numbers to the person responsible for conducting the destruction who will make the appropriate entries on the destruction record.

(c) Immediately after verifying the accuracy and completeness of the material to be destroyed, one person will insert the material into the destructor while the other person watches.

(d) The CMS 25 or equivalent will be used to document the destruction of every segment of keying material from that keylist/book.

c. Loss of keying material. In the event of a possible loss of keying material:

(1) Stop all destruction procedures immediately.

(2) Contact the CMS Custodian immediately, then begin search.

(3) Search entire area.

(4) Recheck all keying material which has been used and the remaining keying material in the card book or key list.

9. CMS Inventories. CMS inventories will be conducted per Chapter 7, paragraph 730 of reference (a). All SF-153 inventories will be conducted by the local account custodian and the primary alternate, or two alternates as per paragraph 730, subparagraph C(4) of reference (a). The original SF-153 will be turned into the custodian for verification. Upon receipt of prepared SF-153 inventories from the local account/alternate, the account custodian will verify it and return an annotated copy. All SF-153 inventories will be stamped "CONFIDENTIAL" at both the top left and bottom right corners. At bottom left corner, type declassification instructions "DECL: OADR." The following inventories will be conducted by the local account user for verification:

- a. Semiannually;
- b. Special - Change of Command, Change of Local Account Users; and
- c. Special, as directed by higher authority.

Users who draw CMS distributed material will maintain and conduct a daily (7 days a week) progressive inventory of material in their custody. In the case of software, this inventory is to be conducted on a watch-to-watch/shift-to-shift basis. For hardware, this inventory is to be conducted a minimum of once a day.

10. Resealing of Primary Keying Material. Extractable (segmented) primary keying material and nonextractable (not segmented) primary keying material that will not be used for a significant period of time, including weekends, will be sealed/ resealed in the following manner:

- a. After page checking the material, place only the effective portions of the keying material in an envelope. All superseded segments must be destroyed prior to sealing material. Take the corresponding local destruction record and note in the right margin next to the last segment destroyed the word "sealed." File the destruction record separately; do not seal it with the material. When the material is reopened, destroy all superseded segments and right below where you indicated the material was sealed, write the word "opened."

- b. When sealing/resealing material the following information must be listed on the outside of the envelope:

- (1) Short Title
- (2) Edition Suffix
- (3) Accountability Legend Code (ALC)
- (4) Classification (front and back of envelope)
- (5) Effective and superseded dates
- (6) Segments/cards contained (e.g., cards 17 through 34)
- (7) Date sealed
- (8) Location of destruction record

c. Sign the envelope along all seams so that opening the envelope will deface the signature.

d. Seal all envelope seams with cellophane tape or the equivalent.

11. Emergency Action Plan. The CMS custodian shall ensure that a detailed emergency action plan for all CMS material is prepared and updated periodically. All local account users will thoroughly familiarize themselves with the provisions set forth in the Emergency Action Plan. In the event an emergency removal is ordered by the Commanding General, the local account/CMS user will remove CMS material by any of the methods approved for routine destruction of COMSEC material. The local account/CMS user will then report the destruction to the CMS custodian. Emergency destruction is not authorized in CONUS. Emergency "removal" will be effected. Per reference (a), annex I, emergency removal is for commands located within the Continental United States (CONUS), planning need consider only nature disasters (e.g., fire, flood, tornado, and earthquake). This includes the removal of COMSEC material to a central location.

12. COMSEC Insecurity. Any actual or suspected loss or compromise of CMS material including two-person integrity violations shall be reported immediately to the CMS custodian. The CMS custodian shall then notify the Staff CMS Responsible Officer and take required action, including the prompt preparation of required reports as outlined in chapter 13 of reference (a).

13. Removal of CMS Material. Under no circumstances will CMS material be removed from this command by anyone other than the CMS custodian or alternate (s).

14. Extracts of CMS Material. Classified CMS material may be reproduced by the CMS account custodian only, and then only per chapter 8, paragraph 850 of reference (a).

15. Action. The CMS custodian shall ensure that CMS administrative personnel and local account understand their CMS responsibilities and that they are sufficiently well trained to carry out those duties. In carrying out this responsibility, the CMS custodian will:

a. Monitor the overall internal security, accountability control and destruction of CMS material and provide oral and written guidance.

b. Review command CMS directives at least annually to ensure their continued accuracy.

c. Ensure, before issuing CMS material to local account that a copy of enclosure (1) is signed and understood (users must only complete enclosure (1)).

d. Ensure that a copy of this instruction, and other command CMS directives are made available to each individual who assumes custody of any CMS material.

  
T. A. CAUGHLAN  
Chief of Staff

DISTRIBUTION: A

StaO 2601.1  
22 AUG 2000

CMS RESPONSIBILITY ACKNOWLEDGEMENT FORM

From: \_\_\_\_\_  
(Rank/Rate, Full Name, SSN, and Command of LE)

To: COMSEC Custodian, \_\_\_\_\_  
(Name of Command)

Subj: CMS RESPONSIBILITY ACKNOWLEDGEMENT

Ref: (a) (CMS 21 and/or the local command instruction governing the handling, accountability, and disposition of COMSEC material. NOTE: the command instruction may contain extracts of CMS-21 that are applicable to LE (e.g., Chapters 6, 8, 11, 13, and 14)).

1. I hereby acknowledge that I have read and understand the reference (a).
2. I assume full responsibility for the proper handling, storage, inventorying, accounting, and disposition of the COMSEC material held in my custody and/or used by me.
3. I have received a copy of the reference from the COMSEC Custodian. 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 COMSEC Custodian and request advice.
4. Before extended departure from the command (i.e., permanent transfer, or leave/TAD/TDY in excess of 30 days) I will report to the COMSEC Custodian and be relieved of responsibility for all COMSEC material that I have signed for.

SIGNATURE: \_\_\_\_\_

DATE: \_\_\_\_\_

NOTE:

1. All Local Element personnel and/or person to whom COMSEC material is issued must complete a CMS Responsibility Acknowledgement Form. This requirement does not apply to individuals who access GPS key via the TAMPS for loading into aircraft.
2. This form will be reproduced locally and the required information will be typed or printed in black or blue-black ink.
3. Retain this form in the Chronological File for a period of 90 days after the date an individual has been relieved of responsibility for COMSEC material that he/she signed for.

ENCLOSURE (1)