UNITED STATES MARINE CORPS
I MARINE EXPEDITIONARY FORCE, FMF
CAMP PENDLETON, CALIFORNIA 92055-5400

I MEFO P5500.2
4 Apr 1989

I MARINE EXPEDITIONARY FORCE ORDER P5500.2

From: Commanding General
To: Distribution List

Subj: Accounting and Transmission of Communications Security Material System

Ref: (a) CMS 4L
(b) CSP 1A
(c) FMFPacO 02230.1D

Encl: (1) LOCATOR SHEET

1. Purpose. To promulgate the procedures for the security and handling of Communications Security Material System (CMS) publications and equipment within this Command in consonance with the references.

2. Cancellation. I MAFO 5500.1E

3. Information. The procedures set forth within this Order are designed to ensure the safe and appropriate handling of materials within the Communications Security (COMSEC) System. Included in the COMSEC System is the responsibility for the custody, transmission handling, and disposal of CMS materials.

4. Action

a. All personnel associated with the security and handling of COMSEC material within this Command are charged with familiarization and strict adherence to the procedures set forth within this Order, the references and all applicable publications.

b. Commanding officers are directed to publish written procedures which not only implement the provisions of this Order and referenced directives, but are also considered applicable to their respective units.

5. Recommendations. Recommendations for improvements to this Order are solicited and should be submitted through the Adjutant.

6. Certification. Reviewed and approved this date.

L. E. AUSTIN
Chief of Staff

DISTRIBUTION: LIST III (less T)

LOCATOR SHEET

Subj: Accounting and Transmission of Communications Security Material System

Location: _____
(Indicate the location(s) of the copy(ies) of this Manual)

ACCOUNTING AND TRANSMISSION OF COMMUNICATIONS
SECURITY MATERIAL SYSTEM

RECORD OF CHANGES

Log completed change action as indicated.

Change Number	Date of Change	Date Received	Date Entered	Signature of Person Entering Change

ACCOUNTING AND TRANSMISSION OF COMMUNICATIONS
SECURITY MATERIAL SYSTEM

CONTENTS

ACCOUNTING AND TRANSMISSION OF COMMUNICATIONS
SECURITY MATERIAL SYSTEM

INTRODUCTION

0001. PURPOSE. To promulgate the procedures and technical instructions for the administration of the Communications Security Material System for this Command.

0002. STATUS. The requirements of these procedures are binding on all Command personnel using Communications Security Material. Any deviation from these procedures must be authorized by Director, Communication Security Material System, Washington, DC.

0003. SCOPE. This Order contains instructions for the issuance, storage, handling, destruction, and reporting of Communication Security Material.

0004. RESPONSIBILITY. The currency, accuracy, modification, and distribution of this Order is the responsibility of the Communication Security Materials System Officer (CMSO) (G-6).

0005. ALLOWANCE. Requests for copies of this Order should be forwarded to the Adjutant.

ACCOUNTING AND TRANSMISSION OF COMMUNICATIONS SECURITY MATERIAL SYSTEM

CHAPTER 1

DEFINITIONS AND RESPONSIBILITIES

ACCOUNTING AND TRANSMISSION OF COMMUNICATIONS SECURITY MATERIAL SYSTEM

CHAPTER 1

DEFINITIONS AND RESPONSIBILITIES

1000. MISSION. The mission of the Communications Security (COMSEC) system is to ensure the proper distribution, handling, control, and security of COMSEC material used to maintain the cryptographic security of communications throughout the Naval Service. As a result, the material governed by the COMSEC system is of certain highly sensitive, classified material, and a limited amount of less sensitive but related materials.

1. Basic Methods of Fulfilling the Mission. As a means of fulfilling its mission, the COMSEC system employs a number of safeguards designed to provide maximum protection against loss or compromise of material within the system. The principle safeguards are listed below and are in force throughout the COMSEC system:

a. Identification of CMS items by short title;

b. Use of accounting numbers (serial numbers, copy numbers) when required;

c. Indication of specific control methods by the use of accountability legends codes (ALC);

d. Maintaining of a continuous chain of custody by the use of transfer reports, local custody documents, and destruction records;

e. Use of specific procedures for the transfer, handling, and storage of CMS material;

f. A central accounting system;

g. The certification of CMS account holdings by periodic inventory;

h. The immediate report of any loss, or compromise.

2. Terms and Abbreviations. The following definitions are provided for general information and understanding of the most frequently used terms and abbreviations used within the COMSEC system:

a. COMSEC - Communications Security;

b. CMS - Communications Security Material System;

c. DCMS - Director, Communications Security Material System. Person and organization responsible for administering CMS within the Department of the Navy.

d. CMIO - COMSEC Material Issuing Office. The distribution point for COMSEC material. Issues material on a periodic basis, usually monthly;

e. CMS Custodian - the person designated by the Commanding General to assume custody, control, and management of all COMSEC material issued to the Command;

f. CMS Alternate Custodian - two person integrity will require the assignment of a minimum of three alternates to compensate for leave, TAD and emergencies. They must have sufficient knowledge and be fully qualified to administer the CMS account in the absence of the CMS custodian;

g. Security Manager - a special staff officer to the Commanding General for the security of all classified material and information within the Command;

h. Local Custody - personal responsibility resulting from the issue of COMSEC material by the CMS Custodian;

i. CMS User - A properly cleared and authorized individual within a command who signs for and receives COMSEC material on a local custody basis and is responsible for its proper handling and use;

j. TPI - Two Person Integrity means that no single person, will at anytime, regardless of grade or status, be allowed access to keying material without the presence of another person formally authorized;

k. Centrally Accountable - material for which reports must be made to DCMS on specific occasions such as transfer, inventory, destruction, or loss;

l. Locally Accountable - material which has been removed from central accountability and is therefore no longer accountable to DCMS, but is still locally accountable to the CMS custodian;

m. Accountability Legend Code (ALC) - The ALC numbers one through five are assigned to all COMSEC material. This code details the method by which the material is accounted. The ALC is assigned on the basis of handling and controlling requirements;

(1) AL-1 is material which is centrally accountable by serial number throughout its life span, from its creation to its destruction;

(2) AL-2 is material which is centrally accountable by quantity only throughout its life span, from production to destruction;

(3) AL-3 is material which is centrally accountable by serial number through local issue then locally accountable only;

(4) AL-4 is material which is administratively CMS controlled for supply purposes and is locally accountable only;

(5) AL-5 is material accountable to DCMS by serial number from Navy receipt to destruction.

n. Reserve On-board (ROB)- material which is not authorized for current use, but is held by the CMS Custodian until it becomes effective;

o. Effective - material which is authorized for current use;

p. Superseded - material for which the authorized usage period has expired;

q. Defense Courier Service (DCS) - The shipping system for COMSEC material.

1001. RESPONSIBILITIES

1. Commanding General. The Commanding General retains overall responsibility for the safeguarding of all classified information within the Command. In addition, the Commanding General retains overall responsibility for the custody, handling, transmission, and disposition of all COMSEC material within the Command CMS account.

2. Security Manager. The Security Manager is the Commanding General's principal advisor in matters pertaining to the security of classified information. In regards to CMS matters the Security Manager will ensure that all security requirements stipulated in the references are followed. Security evaluations/inspections are to be performed by the Security Manager or a designated representative who is familiar with the references. Counter Intelligence assistance will be available upon request.

3. CMS Custodian

a. The CMS Custodian is responsible for making COMSEC material readily available to qualified users. This includes the management

and control of all CMS material held by the command. The CMS Custodian is responsible for issuing material to authorized users and ensuring that recipients are adequately instructed in its proper handling, timely destruction of superseded material, for maintaining accurate records, and preparing and submitting the necessary reports.

b. The CMS Custodian is responsible for monitoring the overall protection, internal security, accountability, and control of CMS material.

c. The CMS Custodian is responsible for establishing written instructions for the users of CMS material.

d. The CMS Custodian is responsible for establishing, reviewing and updating an Emergency Action Plan for CMS material.

e. The CMS Custodian is responsible for establishing and operating a training program for all CMS Users.

f. The CMS Custodian is responsible for establishing and maintaining classification principles and procedures that are in compliance with OPNAVINST 5510.1H, "Information and Personnel Security Program." This means classified information marking, downgrading and declassification actions prescribed in that regulation are applicable to CMS information. However, COMSEC information is handled and controlled in accordance with the references. This may lead to conflict in interpreting which provisions are applicable. Accordingly, the following procedures are established for other classified information integrated within the CMS account.

(1) Classified information received from the Classified Material Control Center (CMCC) and held, within the CMS account will be treated in accordance with CMS directives.

(2) The CMS account will be designated a secondary control point for CMCC materials and comply with command directives governing the control, inspection, and inventory of CMCC information.

(3) The CMS Emergency Action Plan, for use during emergencies such as fire, flood, or other natural disasters, is written and maintained by the CMS Custodian. The plan is designed so that it may be carried out by two properly cleared individuals, and will govern all classified material stored in the CMS account and user areas.

(4) In the case of an emergency (e.g., fire) an authorized person may obtain the second combination to gain access to the vault. Only in this case is this not a security violation. Following such emergency access, a complete inventory will be conducted by the CMS Custodian and alternate and all combinations will be changed.

4. CMS Users. The ultimate success or failure of COMSEC rests with the CMS user. The COMSEC material is worthless if the CMS user is careless or does not follow established procedures for the use, safeguarding, and timely destruction of COMSEC materials. Any CMS user with classified COMSEC material in their possession is directly responsible for its safekeeping. The CMS Custodian will ensure that anyone to whom the CMS Custodian gives the material is authorized to receive it. The CMS user is responsible for adhering to all security rules at all times and for reporting to superiors any circumstances, occurrences, intentional or inadvertent acts which could lead to the disclosure of classified COMSEC information or material to unauthorized persons.

5. PROCEDURES

a. Complete destruction of CMS keying material will be accomplished no later than 12 hours after the supersession. Destruction of keying material which was effective and used over a weekend or holiday period may be extended to a maximum period of 72 hours, effective keying material used during normal week days may not be extended beyond the 12 hours unless approved by the controlling authority.

b. Placement of superseded keying material in a burn bag does not constitute destruction.

c. Complete destruction is destruction by burning, shredding or other authorized means to make reproduction impossible. The cross cut shredder located in the CMS vault, building 1413, room number 141, will be used to destroy all primary keying material for this Command.

d. Areas or spaces which contain cryptographic equipment will be designated RESTRICTED areas. A RESTRICTED area is any area containing classified information which is of such a nature that access to the area constitutes access to classified information. Only persons whose duties actually require access and who have been granted appropriate security clearances will be allowed into RESTRICTED areas. Access lists will be used to control entry into RESTRICTED areas. Entry by an individual not on the access list must be approved by the Commanding General or designated representative in his absence.

CHAPTER 2

CMS PERSONNEL REQUIREMENTS AND DUTIES

CHAPTER 2

CMS PERSONNEL: REQUIREMENTS AND DUTIES

2000. CMS RESPONSIBILITY OFFICER (RO)

1. Requirements. Personnel assigned to be the CMS Responsibility Officer must be designated in writing by the Commanding General. This officer will assume responsibility for routine CMS matters and sign CMS reports "By direction."

2. The CMS RO is a staff assistant to the Commanding General and is directly responsible to him in CMS matters. For emergency and time-sensitive matters the CMS RO will report directly to the Commanding General, keeping the Chief of Staff informed as practical.

3. The CMS RO is responsible for the administration of the CMS account and for ensuring the following:

a. Compliance with established policy and procedures governing the safeguarding and handling of the COMSEC material;

b. Appointment of qualified CMS custodian and alternate custodians;

c. Access to keying material is limited to those authorized in writing;

d. Local training procedures are adequate to meet operational requirements;

e. No other collateral duties are assigned to the CMS custodian and primary alternate custodian;

f. All CMS insecurities and practices dangerous to security are promptly reported and action taken as required;

g. Appropriate action is taken regarding discrepancies noted during CMS training and assistance visits and CMS inspections;

h. Review is made of established local procedures for identifying any potentially significant changes in lifestyle, financial status or disciplinary problems involving personnel authorized access to COMSEC material. Report these changes to the command security manager and if appropriate, the Special Security Officer (SSO);

i. Unannounced spot checks are conducted of the CMS vault and spaces where CMS material is used and stored (see figure 2-1);

j. Management procedures and practices are reviewed with the CMS Custodian and Alternates;

k. Exit briefings are received from Signal Security Advice and Assistance Teams and CMS inspectors upon completion of CMS training and assistance visits and CMS inspections;

l. Comments on the CMS Custodian's and Alternates' performance are included in officer and enlisted fitness reports;

m. All periods of assignment as CMS Custodian, local holder custodian, or alternate are documented in the individual's service record;

n. Emergency Action Plans are established and tested.

2001. CMS CUSTODIAN

1. Requirements. Personnel assigned the billet of CMS Custodian must meet the following requirements:

a. If the CMS Custodian is an enlisted Marine, then the Marine must be a gunnery sergeant or above;

b. If the CMS Custodian is an officer, then that person must have a minimum of six months of active duty service time in addition to the time spent in service schools;

c. The CMS Custodian must have a Top Secret clearance based on a Background Investigation (BI) and updated every four years, six months.

d. The CMS Custodian must have attended the Naval Communication School or be scheduled to attend the Naval Communication School, and a minimum of three years has elapsed between assignments to CMS custodian duties.

e. The CMS Custodian and alternates will not be assigned to the account for more than three years.

f. The CMS Custodian must not have operational control of the section which uses the COMSEC equipment.

2. General Duties

a. The CMS Custodian is responsible to the CMS Responsibility Officer for the proper management of the unit's COMSEC material. The CMS Custodian is the principal advisor to the Commanding General concerning the physical security and handling of COMSEC material, including reports and records. The CMS Custodian's role in the CMS chain of command is as follows:

(1) The CMS Custodian represents the Command in providing guidance concerning CMS, and all CMS users are required to carry out such guidance.

b. Upon the receipt of new manuals or revised manuals, the CMS Custodian shall provide the Commanding General and other interested officers with general information about the contents and impact. This is particularly important with regard to CMS 4L and the Communication Security Publication Memoranda (CSPM).

c. The CMS Custodian will keep the Alternate CMS Custodians informed of Command CMS management systems, location of files, etc., so that the Alternate Custodians are at all times ready to assume the CMS Custodian's duties.

d. The CMS Custodian will conduct appropriate training and provide guidance to Command personnel whose duties include responsibility for COMSEC material or require proper execution of CMS procedures.

e. The CMS Custodian will monitor the overall internal security, accountability, and control of CMS material.

f. The CMS Custodian will establish and maintain written instructions for users of CMS material.

g. The CMS Custodian or Alternate should routinely make spot checks in CMS user area (See figure 2-1).

h. The CMS Custodian will arrange for a Naval Security Group (NAVSECGRU) training visit at least every 18 months. This informal visit provides advice and guidance to personnel who handle COMSEC material and assists in detecting and correcting insecure practices, procedures and communication vulnerabilities. Arrangements for a NAVSECGRU training visit can be made by calling autovon 577-9387 or commercial (619) 437-9387. Preparation for a training visit is required. The CMS Custodian and the CMS Alternate Custodians should be on hand to assist the training visit team on arrival. A NAVSECGRU training visit outline is employed during the conduct of the training visit which covers various topics and lists associated references.

3. Specific Duties. Maintaining TPI, the CMS Custodian will accomplish the following:

a. Become thoroughly familiar with and ensure compliance with the applicable references in order to obtain adequate supplies, and maintain required records concerning CMS material;

b. Draw and maintain on board the required holdings of COMSEC material;

c. Maintain proper storage and physical security;

d. Issue material on a local custody basis to authorized personnel, ensuring that these personnel receive or possess specific written instructions regarding proper storage, handling requirements, local destruction, and accounting procedures. Prior to issuance of COMSEC material, a statement of responsibility for CMS material form will be completed by the user personnel. This statement will be retained on file in the CMS vault;

e. Ensure that CMS Users have ample opportunity to perform corrective and preventive maintenance of COMSEC equipment;

f. Ensure that CMS Users maintain strict accountability for CMS crypto material when it is turned over from one watch to another;

g. Ensure the prompt and proper entry of all amendments to COMSEC publications and equipment by qualified personnel in accordance with existing instructions;

h. Ensure the completeness of material by conducting page checks of all publications and repair kits or by causing them to be conducted during every inventory;

i. Comply with authorized methods and procedures for the destruction of COMSEC material;

j. Maintain the Command Standing Operating Procedures and Emergency Action Plan, ensuring that the plans are up-to-date, practical, and thoroughly understood by all individuals who will be responsible for using them;

k. Provide for the prompt and accurate preparation, signing, and submission of CMS correspondence, messages, and reports, and ensure that the Command's CMS account number is on all CMS correspondence, messages, and reports;

l. Conduct required inventories;

m. Maintain adequate physical security measures when transporting CMS material to and from the DCS pickup point; and,

n. Report immediately to the Commanding General or CMS Responsibility Officer any suspected compromise, loss, unauthorized destruction, or finding of material.

4. <u>Change of Custodian</u>

a. The CMS Custodian will be designated in writing in accordance with Article 301 of CMS 4L.

b. The newly appointed CMS Custodian will conduct and sight inventory all accountable CMS material. The CMS Custodian being relieved will witness this inventory, except when the CMS Custodian has been detached from the Command or is otherwise unable to perform the task. The inventory will be conducted in accordance with Article 1001 of reference (a).

2002. ALTERNATE CMS CUSTODIAN

1. Requirements. The requirements for personnel serving as Alternate CMS Custodians are the same as the requirements for the CMS Custodian.

2. Appointment. The Alternate CMS Custodians are appointed in writing in accordance with the instructions set forth in Article 301 of CMS 4L. There must be a minimum of three alternates designated in writing.

3. Readiness to Assume the Duties of Custodian. The Alternate CMS Custodians will be thoroughly familiar with the references pertaining to the COMSEC Material System and the procedures set forth in this Order. In addition, the Alternate CMS Custodians will keep themselves informed of Command CMS management procedures, the location of the files, etc., so that the Alternate CMS Custodians will remain ready to assume the duties of the CMS Custodian at all times.

2003. CMS USERS

1. Requirements. A CMS user is any properly cleared and authorized individual who signs a local custody document accepting local custody responsibility from the CMS Custodian. Unlike the CMS Custodian, a CMS user is not a management representative of the Commanding General, but is tasked with the operational execution of approved handling and control procedures as directed by the CMS Custodian. By the CMS users' signature, the CMS user indicates the awareness of TPI requirements for proper handling, safeguarding, and control as well as requirements for conducting or supervising local destruction as appropriate and as authorized.

2. Training and Designation. All CMS users will all be trained and designated in accordance with the procedures established by the CMS Custodian. Written designation is not required by the Director, COMSEC Material Systems (DCMS) but as a matter of Command policy, all Users will be designated by letter; e.g., figures 2-2 and 2-3. The CMS user is required to complete a statement of responsibility prior to the issuance of COMSEC material, (see figure 2-4) and to have in their possession Figure 2-5, Foolproof CMS User Handling Instructions.

3. Requirement for Signature. All accountable CMS material located in a space not under the operational control of the CMS Custodian, will be signed out to a CMS User. Further, CMS Users will comply with the technical and managerial guidance provided by the CMS Custodian.

4. Handling Procedures. Handling of COMSEC material is those actions done by cleared personnel to obtain, store, use, return, and destroy COMSEC material. This includes the use of local custody documents, CMS destruction records, and local storage safes.

a. Upon receiving any COMSEC material, the CMS users will verify the material by title, serial number, edition, and check to ensure the items are complete. This includes page checking all key lists and publications.

b. The TPI material subcustodied to users will require two signatures for all material received on the appropriate forms; e.g., figures 2-6 and 2-7.

c. Complete destruction of CMS keying material will be accomplished no later than 12 hours after the supersession. Destruction of keying material which was effective and used over a weekend or holiday period may be extended to a maximum period of 72 hours, effective keying material used during normal week days may not be extended beyond the 12 hours unless approved by the controlling authority.

d. All keying material issued will have a local destruction record included. As material is destroyed, it should be recorded on the CMS 25 Form Destruction Record, (see figure 2-8). This record and the residue material should be turned into the CMS Custodian on the first day of the month following the effective month. In all cases the residue material and Destruction Report will be turned in to the CMS Custodian before the fourth day of the month following the effective month.

e. All COMSEC equipment will be turned in to the CMS Custodian as soon as possible after it is no longer needed.

f. When the CMS user turns in material residue and local destruction records or equipment, the CMS Custodian will check reports for correct use and completeness of equipment as well as correct serial numbers and sign the material back into the vault.

g. The careful handling and safeguarding of COMSEC material and equipment cannot be overemphasized. A person who has signed for COMSEC material has acknowledged responsibility for the proper safeguarding of the material and agrees to insure that those authorized personnel utilizing the material are properly briefed on its handling and two person integrity.

5. Storage Procedures. The storage of COMSEC material will provide maximum protection from compromise, loss, damage, and access by unauthorized personnel.

a. All Top Secret cryptographic material will be stored in a Class B vault or a class 2, 4, or 5 steel, GSA approved safe with a tumbler, manipulation proof combination lock.

b. All Secret cryptographic material will be stored as required for Secret and Top Secret material or in a Class C vault, or in a GSA approved safe.

c. Confidential cryptographic material will be stored as required for Secret or Top Secret material or in a Class C vault, or in a GSA approved safe.

d. Additional details on appropriate security containers for storing classified material can be found in the current edition of OPNAVINST 5510.1.

e. Combinations to all safes will be changed at least semi-annually, whenever a person having safe access is transferred, or when the combination becomes known to an unauthorized person.

f. All safes and vaults containing COMSEC material will have a safe or cabinet Security Record posted on the inside of the container, (see figure 2-9).

g. Security Container Information Standard Form 700, Figure 2-10, is to be placed inside of the security container. Responsible users are required to keep this form updated for home address and phone numbers for recall purposes. If the container is found unlocked after normal working hours, the personnel listed would be recalled.

h. Combination envelopes to all CMS User's safes will be filed with the CMS Custodian located in room 141, building 1413. The CMS vault combination envelope will be on file in the CMCC office in Building 1133.

i. Secure all classified material, lock all security containers, and check working space for classified material when leaving office space during working hours and prior to securing each day. After security check is completed, initial Activity Security Checklist, Figure 2-11.

j. A copy of the CMS Emergency Action Plan will be placed on the container for the safeguarding of cryptographic material in the event of any circumstance where there is a danger of classified material being compromised.

k. All COMSEC material will be properly safeguarded when not in use.

l. Personnel responsible for handling classified cryptographic material or equipment will exercise the highest degree of personal initiative to insure that the possibility of compromise is precluded.

ACCOUNTING AND TRANSMISSION OF COMMUNICATIONS
SECURITY MATERIAL SYSTEM

CMS SPOT CHECK

Date: _____

User area checked: _____

Spot check conducted by: _____
(Name) (Rate/Rank) (Position/Title)

Spot check conducted with: _____
(Name) (Rate/Rank) (Position/Title)

Discrepancies: (if any) _____

Corrective action/training provided: _____

Follow-up spot check required: _____
(Date)

NOTE: For properly documented training, the name/signature of the individual(s) being trained is required. If it's not documented, it didn't happen.

Figure 2-1.-- CMS Spot Check Checklist.

ACTIVITY (CMS User Area)	DATE

RECEIPT AUTHORIZATION RECORD NCSCP 5511/1 (10-61) *(Print or type entries)*

1. Persons whose names and signature appear below are authorized to receipt for classified material directed to this office.
2. It is certified that these persons have the clearance and access shown below.
3. All previous authorizations are hereby cancelled.

NAME	RANK	HIGHEST CLASSIFICATION	SIGNATURE
(Typed name, SSN)			

AUTHORIZING OFFICIAL (CMS Responsible Officer)	SIGNATURE
ACTIVITY (CMS User Area)	DATE

Figure 2-2.--Authorization for Access to CMS Material/Individual Access Update.

ACCOUNTING AND TRANSMISSION OF COMMUNICATIONS
SECURITY MATERIAL SYSTEM

CMS RESPONSIBILITY ACKNOWLEDGMENT FORM

From: _____
(Printed Name of Individual, Rate/Grade, and SSN)

To: CMS Custodian

Subj: CMS RESPONSIBILITY ACKNOWLEDGMENT

Ref: (a) I MEFO P5500.2
(b) Foolproof CMS User Handling Instructions

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

2. I assume full responsibility for the proper handling, storage, inventory, accounting, transfer, and destruction of CMS material held in my custody and/or used by me or those under my supervision.

3. I have received instructions in the handling of CMS distributed material from the CMS Custodian. If at any time I am in doubt as to the proper handling of CMS material, I will immediately contact the CMS Custodian and request advice.

4. Before departure on leave, TAD, or detachment from the command, I will check out with the CMS Custodian.

SIGNATURE _____

DATE _____

Figure 2-4.--Statement of Responsibility for CMS Users.

ACCOUNTING AND TRANSMISSION OF COMMUNICATIONS
SECURITY MATERIAL SYSTEM

CMS RESPONSIBILITY ACKNOWLEDGMENT FORM

From: _____
(Printed Name of Individual, Rate/Grade, and SSN)

To: CMS Custodian

Subj: CMS RESPONSIBILITY ACKNOWLEDGMENT

Ref: (a) I MEFO P5500.2
(b) Foolproof CMS User Handling Instructions

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

2. I assume full responsibility for the proper handling, storage, inventory, accounting, transfer, and destruction of CMS material held in my custody and/or used by me or those under my supervision.

3. I have received instructions in the handling of CMS distributed material from the CMS Custodian. If at any time I am in doubt as to the proper handling of CMS material, I will immediately contact the CMS Custodian and request advice.

4. Before departure on leave, TAD, or detachment from the command, I will check out with the CMS Custodian.

SIGNATURE _____

DATE _____

Figure 2-4.--Statement of Responsibility for CMS Users.

ACCOUNTING AND TRANSMISSION OF COMMUNICATIONS
SECURITY MATERIAL SYSTEM

1. DESTRUCTION OF CMS MATERIAL

a. By far the most important duty a CMS user will have while in the field in possession of CMS primary keying material or authentication devices is the proper handling and recording of the destruction of the same.

b. The destruction of CMS material is a simple process of recording everything you destroy, each segment, each day, of each short title signed out.

c. The witness for destruction, and the individuals who sign the destruction report must include the person who signed for the material on the subcustody document and any other properly cleared person, military or civilian with a classification equal to or higher than the material being destroyed.

d. Upon return from field operations, the CMS user must turn in either the CMS material or properly completed CMS 25 destruction form completed by two witnesses.

e. Time periods for the destruction of CMS software are based on the classification and type, not accountability legend code.

(1) Keying material hardcopy form (tape, cards, or settings to be used with secondary variables) marked "CRYPTO" is the most sensitive element in providing communications security. This material must be destroyed as soon as possible after supersession and always within 12 hours unless the material is sealed. Superseded segments of sealed segmented/extractable keying material need not be destroyed until the entire edition is superseded or the keying material is unsealed, whichever occurs first. Citing an example, if a book of keycards is unsealed on the 16th of the month , segments/days 1-15 must be immediately destroyed and recorded as such. In the event a single day has been compromised and an emergency supersession is declared by the operational controller of that keylist for that day the material must be unsealed and all superseded segments destroyed at that time. If day 15 was compromised, and an emergency supersession is declared and your book of keycards is still sealed you would have to open your keying material and destroy day 15 and all superseded segments.

(2) All other COMSEC material (publication, microfiche, and keying material in hard copy form but not marked CRYPTO) must be destroyed within five days after supersession.

Figure 2-5.--Foolproof CMS User Handling Instructions.

f. If you used day 1, destroy and record it immediately or within 12 hours after you go to day 2.

g. REMEMBER, IF YOU DESTROY IT, RECORD IT!

2. STORAGE OF CMS MATERIAL

a. Shore stations

(1) Top Secret keying material shall be stored in a Class 1, 2, 4 or 5 GSA approved security container which requires two person integrity to open.

(2) Secret keying material shall be stored in any GSA approved security container which requires two person integrity to open.

(3) Confidential material not marked "CRYPTO" shall be stored in a file cabinet having an integral automatic locking mechanism and a built-in three-position manipulation-resistant, dial-type, combination lock, or any container approved for storing Secret or Top Secret material.

b. While aboard Navy ships

(1) Top Secret keying material shall be stored in a steel filing cabinet having a Group 1 or Group 1R combination lock, or in a strong room, or in any storage container approved for storing of Top Secret keying material at shore stations. Any storage container used must require two person integrity to open.

(2) Secret keying material shall be stored in a steel-security filing cabinet having a lockbar secured by an approved three-position, dial-type, combination padlock procured from the Federal Safety Supply Schedule, or in a strong room, or in any storage container approved for storing of Secret or Top Secret keying material aboard ships. Any storage container used must require two person integrity to open.

(3) Confidential material not marked "CRYPTO" may be stored in a standard field safe, or any similar security padlock which meets Federal Specifications. Confidential material marked "CRYPTO" shall be stored in the same manner as Secret keying material.

3. PAGECHECK REQUIREMENTS

a. Pagechecks of unsealed primary keying material must be accomplished upon initial receipt, during daily watch-to-watch

Figure 2-5--Foolproof CMS User Handling Instructions--Continued.

inventory and upon destruction by the two persons witnessing the burn. Sealed primary keying material must be pagechecked upon opening.

b. Unsealed administrative, maintenance, and operating instructions must be pagechecked upon receipt from I MEF CMS.

c. Sealed primary keying material should not be opened for the sole purpose of conducting a pagecheck until 72 hours of anticipated use. A pagecheck shall be conducted when opening sealed keying material.

d. Sealing Segmented Keying Material to avoid pagechecks--If all or part of an edition of extractable primary keying material, except key tapes packaged in canisters, will not be used for a significant period of time, the effective and future portions of the material may be sealed in accordance with the following procedures.

(1) After pagechecking the material, place the effective and future use segments of the keying material in an envelope. All segments superseded prior to the date the material is sealed must be destroyed immediately and their destruction properly recorded on the existing CMS 25 record that is stored separately from the material.

(2) On the outside of the envelope, list the short title, edition suffix, (if any), accounting (serial) numbers, accountability legend code, classification status of the material, which days are enclosed, date sealed and location of the local destruction record.

(3) Sign the envelope along its principal seams so that opening the envelope will deface the signature.

(4) Seal all seams with cellophane tape or the equivalent. Masking tape is not to be used.

(5) When keying material sealed in the above manner is opened, the material must be pagechecked and all superseded segments must be removed and destroyed immediately. The destruction of superseded segments from locally sealed materials must be contained on the CMS 25 Destruction Record regardless of whether destruction of the entire edition will be summarized later on an SF-153 of CMS 2-1A/2-3.

NOTE: Local destruction pages printed on/with the key card book are no longer authorized for recording destructions. The CMS 25 must be utilized.

Figure 2-5.--Foolproof CMS User Handling Instructions--Continued.

4. CMS USERS AND WITNESSES

a. When submitting access cards to I MEF CMS, the user's Section Head must ensure all personnel meet the following requirements. Access cards can be obtained from I MEF CMS.

(1) Natural born or naturalized citizen.

(2) Immigrant aliens lawfully admitted to the U.S. and who are U. S. Government civilian or military employees.

(3) Natural born or naturalized U.S. citizens must have a security clearance equal to or higher than the classification of the material involved. Lawfully admitted immigrant aliens with a final clearance based on a background investigation may have access to COMSEC material classified no higher than Confidential.

(4) Foreign nationals shall not be allowed access to COMSEC material.

b. All CMS witnesses for CMS inventories or destructions will be responsible for the following.

(1) The accuracy of the information listed on the report or record.

(2) The physical sighting of all material inventoried.

(3) The physical sighting of all material to be destroyed and the actual destruction of the material.

(4) The timeliness and validity of the report or record.

Figure 2-5.--Foolproof CMS User Handling Instructions--Continued.

ACCOUNTING AND TRANSMISSION OF COMMUNICATIONS
SECURITY MATERIAL SYSTEM

Date

From: CMS Custodian

To: _____

Witness: _____

SHORT TITLE	QTY	ACCOUNTING NO'S BEGINNING	ENDING	AL

I, the person whose signature appears below, certify that I have in my possession and hold myself responsible for the COMSEC material listed above, commencing on the date indicated, and that I understand the requirements for safeguarding the same.

_____ _____
Date of receipt Signature of Recipient

_____ _____
Signature of Custodian Signature of Witness

- -

Material/Destruction Records Local returned on _____
Date of Return

_____
Signature of Custodian

Figure 2-6.--Local Custody Form

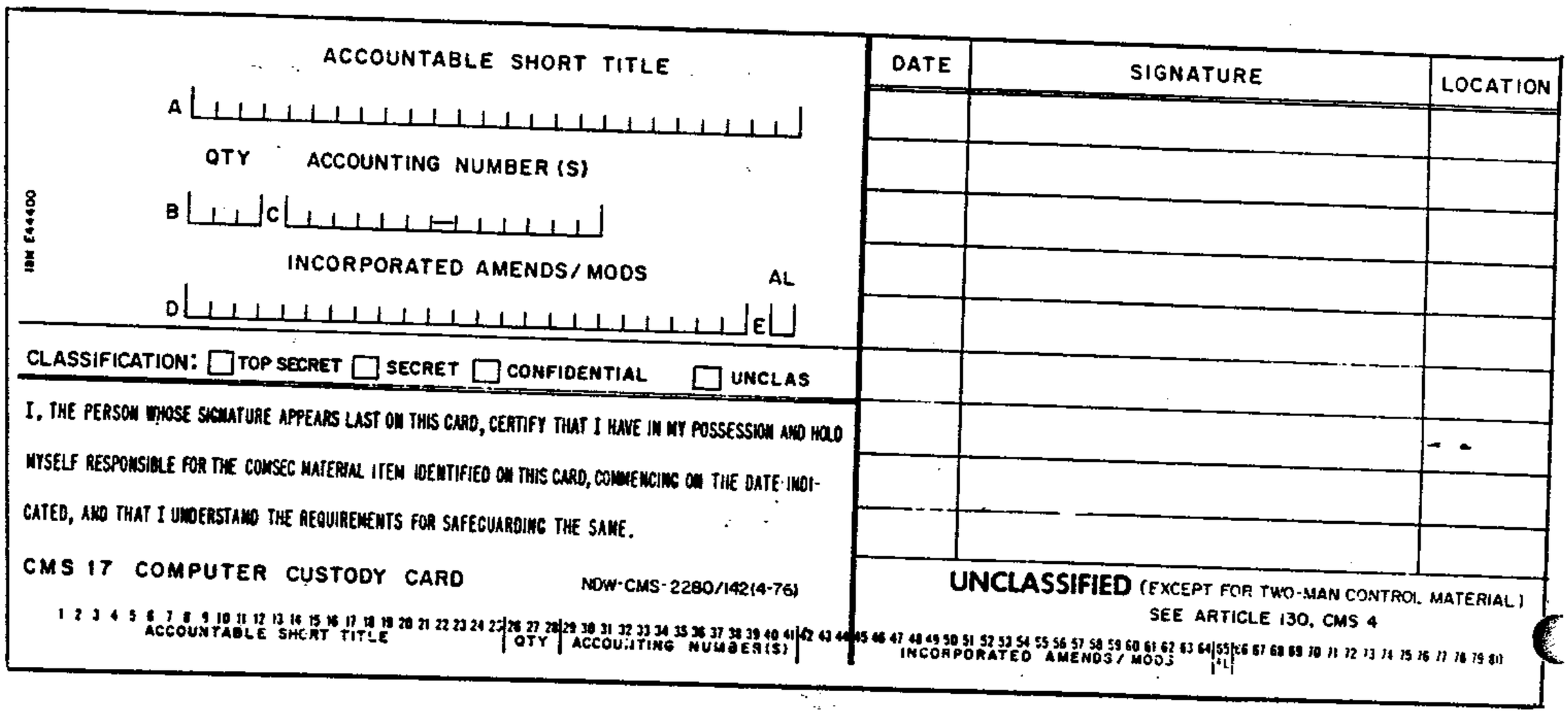

Figure 2-7.--Computer Custody Card

CONFIDENTIAL (When Filled In)

CMS 25

ONE-TIME KEYING MATERIAL DESTRUCTION REPORT

Retain this form locally in the CMS file. See Chapter 9, CMS 4 for instructions on destroying one-time keying material.

These individual one-time keying material cards or segments were destroyed on the dates and by the two individuals indicated below:

Card No.	Date of extract	Signature	Signature	Date destroyed
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				

(Continued)

SHORT TITLE REG. NO./ACCOUNTING NO. AL

CLASSIFIED BY NACSI 4003.

DECLASSIFY ON: ORIGINATING AGENCY'S DETERMINATION REQUIRED.

CONFIDENTIAL (When Filled In)

NDW-CMS-2280/82 (Rev. 11/82)

Figure 2-8.--One-Time Keying Material Destruction Report

SECURITY CONTAINER RECORDS FORM
OPNAV FORM 5510/21 (10-70) S/N 0107-LF-783-8100

CONTAINER NUMBER	LOCATION	OFFICE CODE	TYPE OF CONTAINER (MAKE/SIZE)
DATE RECEIVED	CLASS OF CONTAINER ☐ CLASS 2 ☐ CLASS 3 ☐ CLASS 4 ☐ CLASS 5 ☐ CLASS 6		FEDERAL STOCK NUMBER
SERIAL NUMBER	DATE OF MANUFACTURE	QUANTITY OF DOCUMENTS	SCOPE OF MATERIAL
SECURITY POINTS FOR CONTAINER	OTHER SECURITY POINTS		TOTAL SECURITY POINTS

PERCENTAGE OF CLASSIFIED MATERIAL STOWED

TOP SECRET % SECRET % CONFIDENTIAL % UNCLASSIFIED %

TYPE OF LOCK (MAKE/MODEL)	SERIAL NUMBER (IF APPLICABLE) HASP	LOCK CASE
CONDITION OF CONTAINER		

REMARKS

OPNAV FORM 5510/21 (10-70) (BACK)

INSPECTION AND REPAIR

DATE INSPECTED	INSPECTED BY	CONDITION	REPAIRS MADE/DRILLED

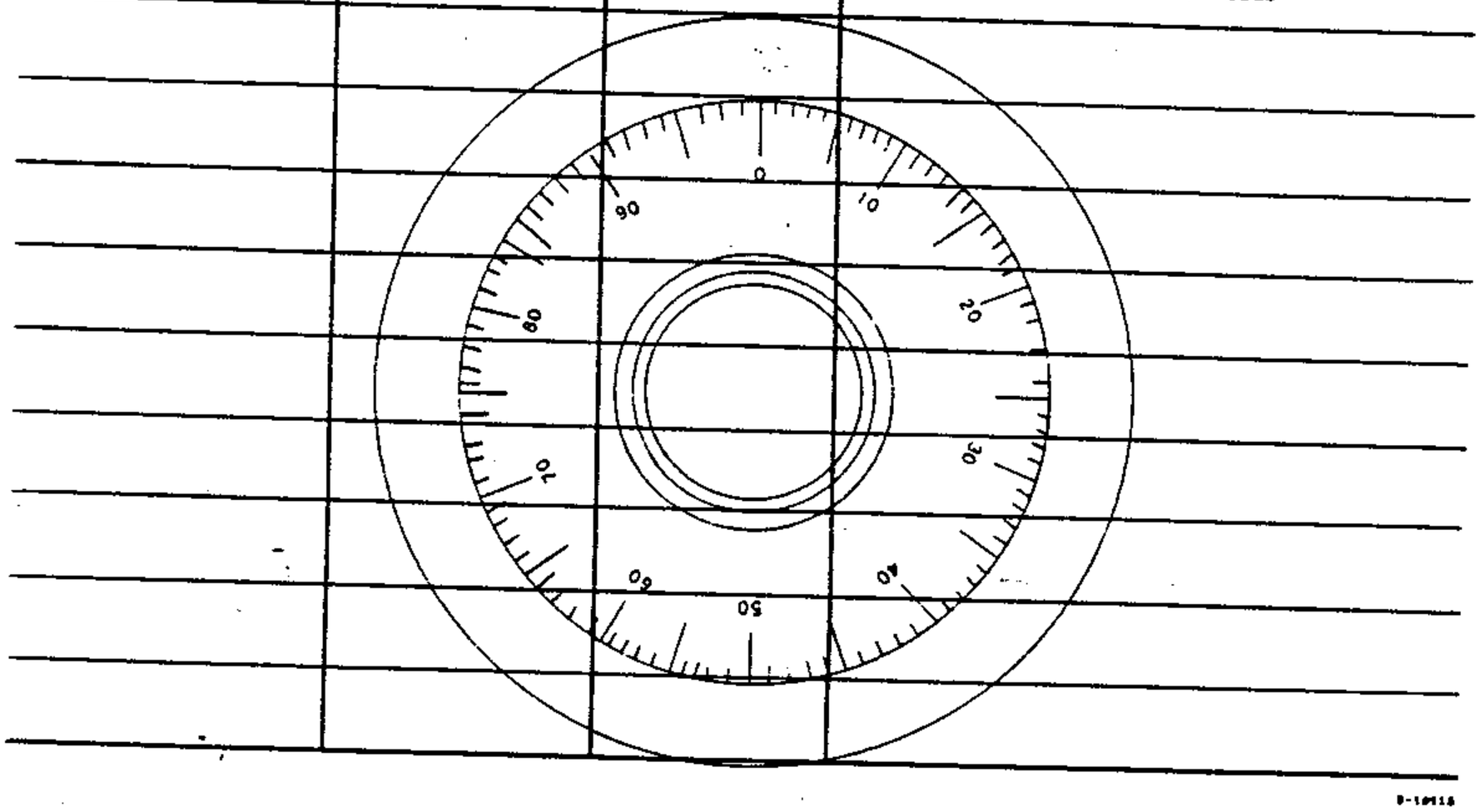

Figure 2-9.--Security Container Records Form

SECURITY CONTAINER INFORMATION

INSTRUCTIONS

1. COMPLETE PART 1 AND PART 2A (ON END OF FLAP).
2. DETACH PART 1 AND ATTACH TO INSIDE OF CONTAINER.
3. MARK PARTS 2 AND 2A WITH THE HIGHEST CLASSIFICATION STORED IN THIS CONTAINER.
4. DETACH PART 2A AND INSERT IN ENVELOPE.
5. SEE PRIVACY ACT STATEMENT ON REVERSE.

1. AREA OR POST (If required)	2. BUILDING (If required)	3. ROOM NO.
4. ACTIVITY (DIVISION, BRANCH, SECTION OR OFFICE)		5. CONTAINER NO.
6. MFG. & TYPE CONTAINER	7. MFG & TYPE LOCK	8. DATE COMBINATION CHANGED
9. NAME AND SIGNATURE OF PERSON MAKING CHANGE		

10. Immediately notify one of the following persons, if this container is found open and unattended.

EMPLOYEE NAME	HOME ADDRESS	HOME PHONE

1. ATTACH TO INSIDE OF CONTAINER

700-101
NSN 7540-01-214-5372

STANDARD FORM 700 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

WARNING

WHEN COMBINATION ON PART 2A IS ENCLOSED, THIS ENVELOPE MUST BE SAFEGUARDED IN ACCORDANCE WITH APPROPRIATE SECURITY REQUIREMENTS.

DETACH HERE

CONTAINER NUMBER

COMBINATION

_____ turns to the (Right) (Left) stop at _____
_____ turns to the (Right) (Left) stop at _____
_____ turns to the (Right) (Left) stop at _____
_____ turns to the (Right) (Left) stop at _____

WARNING

THIS COPY CONTAINS CLASSIFIED INFORMATION WHEN COMBINATION IS ENTERED.

UNCLASSIFIED UPON CHANGE OF COMBINATION.

2A INSERT IN ENVELOPE

SF 700 (8-85)
Prescribed by
GSA/ISOO
32 CFR 2003

Figure 2-10.--Standard Form 700

ACTIVITY SECURITY CHECKLIST

DIVISION/BRANCH/OFFICE | ROOM NUMBER | MONTH AND YEAR

Irregularities discovered will be promptly reported to the designated Security Office for corrective action.

Statement

I have conducted a security inspection of this work area and checked all the items listed below.

TO *(If required)* | FROM *(If required)* | THROUGH *(If required)*

ITEM	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1. Security containers have been locked and checked.																															
2. Desks, wastebaskets and other surfaces and receptacles are free of classified material.																															
3. Windows and doors have been locked (where appropriate).																															
4. Typewriter ribbons and ADP devices (e.g., disks, tapes) containing classified material have been removed and properly stored.																															
5. Security alarm(s) and equipment have been activated (where appropriate).																															
INITIAL FOR DAILY REPORT																															
TIME																															

701-101
NSN 7540-01-213-7899

U.S. GOVERNMENT PRINTING OFFICE: 1988-461-275/20198

STANDARD FORM 701 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

Figure 2-11.--Activity Security Checklist

ACCOUNTING AND TRANSMISSION OF COMMUNICATIONS
SECURITY MATERIAL SYSTEM

CHAPTER 3

ACCIDENTAL EMERGENCY ACTION PLAN

CHAPTER 3

ACCIDENTAL EMERGENCY PLAN

3000. GENERAL. This Accidental Emergency Plan consists of two parts, a fire bill and a natural disaster plan. Three types of emergency actions may be taken in the event of an accidental emergency: securing the material, transferring the material, or removing the material. Within the CMCC/CMS strongroom are emergency action cards which detail step by step instructions for each of these actions. These cards, in conjunction with the broad guidance of this chapter and the basic order, shall guide all emergency actions.

3001. FIRE BILL

1. General

(a) Upon arrival of the fire department, do not interfere with fire department personnel or prevent them from approaching or entering the building.

(b) Under no circumstances will personnel needlessly endanger themselves by fighting a fire which is beyond their control.

2. Procedures

(a) Sound the alarm within the I MEF Command Element by setting off the fire alarm.

(b) Call the fire department (911).

(c) Get assistance and attempt to fight the fire. Do not attempt to fight a fire which is beyond control.

(d) Notify the 12/14 Area OOD to establish perimeter around the I MEF Command Element.

(e) Determine whether transfer or removal of classified material is warranted or possible. If possible, do so. If not, immediately secure all safes. Attempt to take all inventories out of the vault so that a proper inventory may be conducted after the fire is extinguished. The CMCC inventories are located under the counter in the main office; CMS inventories are located in the inner vault and need not be removed if the vault door is locked.

(f) After the fire is extinguished, conduct an immediate inventory of any surviving material and report destruction, loss of control or unauthorized viewing of all material to the appropriate authority.

3002. NATURAL DISASTERS. Follow the procedures outlined in Chapter 4, figure 4-2, for the protection of classified material.

SECURITY MATERIAL SYSTEM

CHAPTER 4

EMERGENCY ACTION PLAN FOR CMS/CMCC STRONGROOM

FIGURE

CHAPTER 4

EMERGENCY ACTION PLAN FOR CMS/CMCC STRONGROOM

4000. GENERAL

1. Purpose. To set forth instructions for actions to be taken for the safeguarding, transfer, or removal of classified material located in this organization's CMS/CMCC strongroom.

2. Information. In the event of an accidental emergency this order provides guidance for the safeguarding, transfer, or removal of classified material to preclude its loss or compromise. In all cases, safety of personnel is the first concern. Material which is lost or compromised presents little threat if it is properly reported. If this plan can be implemented without danger to personnel, do so; if not, report the loss or compromise, suspected or confirmed, immediately so that it may be reported to higher authority. The figures to this plan contain general outlines of the procedures to be followed in the event of an emergency. Emergency action cards located inside the CMS/CMCC strongroom detail the exact actions required to implement this plan. Whenever an emergency exists, the person initiating implementation of this plan shall immediately follow the procedures outlined in in figure 4-2. After assessing the situation, he shall proceed with the actions detailed in figures 4-1, 4-3, 4-4, 4-5, 4-6, or as appropriate.

3. Authorization to Implement. If the Commanding General is not available, the senior individual present may implement this plan and any other orders which may be established and to deviate from established plans when circumstances warrant. Preferably, the individual implementing this plan will be the CMS Custodian, Alternate CMS Custodian, or Command Duty Officer. The Commanding General, Chief of Staff or Adjutant will be notified of any emergency actions taken as soon as possible.

4. Basic Emergency Definitions. An emergency is any unforeseen occurrence which results in a significantly increased danger to classified material for a limited period of time.

a. Accidental Emergencies. Fire, collision, flood, or a natural disaster (e.g., tornado, hurricane, tidal wave, etc.)

b. Hostile Action Emergencies. Enemy attack, mob action, bomb threat, terrorist activity, or civil uprising.

c. Safeguarding. When it has been determined that an emergency exists, it may be determined that a greater degree of security for classified materials is desirable. Steps to enhance the security of the CMS/CMCC strongroom are outlined in figure 4-2.

d. Transfer. When it has been determined that an emergency exists, it may become necessary to transfer classified material to an unaffected command for securing of the material. This material is formally placed on charge to the receiving command, and the transfer may be temporary or permanent, depending upon the duration of the emergency. Steps to transfer classified material are outlined in Chapter 3, paragraph 3001.2(e).

e. Removal. When it has been determined that an emergency exists, it may become necessary to remove classified material and store it in a secure area either under this organization's control or under the control of another organization. Removal is a temporary measure only. The material removed remains on charge to this organization. Procedures for the removal of classified material are outlined in figure 4.3.

f. Emergency Destruction. When it has been determined that an emergency exists, it may become necessary to destroy classified material. Usually destruction will only be authorized in instances where transfer or removal is not feasible or where the risk of compromise or loss is imminent. As an emergency develops, particular precautionary destruction or non-mission essential materials may be directed. If the situation warrants complete destruction, all classified materials will be destroyed. In any case, records of what was destroyed are essential to the proper reporting of the incident and the individual in charge of the implementation of this plan must ensure that accurate records are maintained as the destruction proceeds. Destruction of material should be considered only after all reasonable effort has been made to safeguard, remove, or transfer the material.

g. Two Person Integrity (TPI). This is the security measure taken to prevent single person access to COMSEC keying material and cryptographic maintenance manuals. TPI can be accomplished by the constant presence of two authorized persons.

4001. DESTRUCTION

1. Priority of Destruction.

a. Partial Precautionary Destruction Priority. Partial precautionary destruction is the destruction of COMSEC material that is not essential to current operations. The primary value of partial precautionary destruction, once accomplished, is the relative ease and speed of carrying out complete destruction if it should become necessary. The following priorities are established for precautionary destruction:

(1) Superseded Keying Material

(a) Superseded TOP SECRET primary keying material.

(b) Superseded SECRET, CONFIDENTIAL, and UNCLASSIFIED primary keying material.

(c) Superseded secondary variables.

(2) Reserve on Board Keying Material for Use More than One Month in the Future. This category includes all material which is authorized for use after the end of the next month. For example, if a partial precautionary destruction were to occur on 14 July, ROB material scheduled for use in September and succeeding months would be destroyed. ROB keying material shall be destroyed in the same priority order as the superseded categories list in paragraph (1)(a) above.

(3) Non-Essential Classified Manuals. Classified manuals not essential for continuing operations shall be destroyed in the following order:

(a) Maintenance manuals.

(b) Operating manuals.

(c) Administrative manuals.

b. Complete Emergency Destruction Priorities

(1) Keying Material

(a) All superseded primary keying material designated CRYPTO and all TOP SECRET and SECRET tactical operations codes and authentication systems.

(b) Effective primary and secondary variable keying material designated CRYPTO (including keying variables stored electronically in CRYPTO equipment).

(c) ROB TOP SECRET multiholder keying material designated CRYPTO which will become effective within the next 30 days.

(d) Superseded CONFIDENTIAL and UNCLASSIFIED tactical operating codes.

(e) ROB SECRET and CONFIDENTIAL multiholder keying material designated CRYPTO which will become effective in the next 30 days.

(f) All remaining classified keying material, authentication systems, maintenance and sample keys, ROB two holder keying material, and ROB one-time pads.

(2) Manuals and Classified COMSEC Aids. COMSEC material other than keying material or equipment (e.g., maintenance manuals, operating innstructions, and general doctrinal publications) must be kept from unauthorized individuals because they contain information which concerns U. S. crypto systems, the level of cryptographic technical achievements, and the ways in which COMSEC operations are organized and conducted. Some of these manuals have pages which are especially sensitive and which therefore take priority in destruction procedures. Destruction priorities for these classified materials:

(a) Crypto maintenance manuals or their sensitive pages (KAMS).

(b) General doctrinal guidance publications (e.g., AMSG's).

(c) Status documents showing the effective dates for COMSEC keying material (e.g., CSPM-3).

(d) Remaining classified pages of crypto maintenance manuals.

(e) Cryptographic operating instructions (KAO's).

(f) Remaining classified COMSEC documents.

(3) Equipment. While reasonable efforts should be made to evacuate COMSEC equipment, in an emergency the immediate goal of destroying COMSEC equipment is to render it unusable and unrepairable. If time permits, the equipment's cryptologic capability should be destroyed beyond reconstruction. The classified portions of the equipment, which will include components such as printed circuit boards and multilayer boards, keyed permuting devices, and secondary variables such as CRIB's and rotors, should be removed first and destroyed. The destruction priorities for COMSEC equipment are as follows:

(a) Zeroize the equipment if the keying element cannot be physically withdrawn.

(b) Remove and destroy readily removable classified elements, (e.g., printed circuit boards).

(c) Destroy remaining elements. After all classified elements have been destroyed, it is not necessary to destroy the remainder of the equipment.

(4) Combined Complete Destruction Priorities. In cases

where personnel and facilities are limited, the following overall emergency destruction priority list should be followed:

(a) All superseded and effective keying material designated CRYPTO (including keying variables stored electronically in crypto equipment) and all TOP SECRET and SECRET tactical operating codes and authentication systems, ROB two holder keying material, and ROB one-time pads.

(b) All rotors and CRIB's.

(c) Superseded CONFIDENTIAL and UNCLASSIFIED tactical operating codes.

(d) Complete COMSEC equipment maintenance manuals or sensitive pages thereof.

(e) Classified general COMSEC doctrinal guidance publications.

(f) Classified elements of COMSEC equipment.

(g) Remaining COMSEC equipment maintenance manuals and classified operating instructions.

(h) Remaining classified COMSEC material.

(i) Classified message files and classified documents.

(j) General message files.

(k) Naval warfare publications library.

2. Methods of Destruction

a. Combustible Material. Keying material and other classified material must be destroyed beyond reconstruction. Burning material in braziers or burn barrels is the preferred method of destruction. Care should be taken to ensure that all material is completely burned and that the ashes are scattered.

b. Equipment. The classified components of noncombustible crypto equipment and variables must be destroyed as completely as possible and at least beyond immediate re-use. An incendiary equipment destroyer, an incinerator, or a large disintegrator may be used if available; however the probable tool for destruction will be a hammer.

c. Aboard Ship

(1) In the event the ship is in imminent danger of

sinking or is about to be scuttled in either deep or shallow water which the United States controls or can patrol, classified material should not be jettisoned. Crypto equipment will be zeroized and all material will be locked in security containers or vaults, and allowed to sink with the ship.

(2) In the event the ship is in imminent danger of sinking in an area where a foreign power would have salvage opportunities, COMSEC equipment should be zeroized and all material should be completely destroyed. Material which has been only partially destroyed will be jettisoned only if the Captain of the ship directs.

(3) In the event of jettisoning, material wrapped in plastic or otherwise sealed with a slit to avoid the possibility of floatation after the weighted canvas bag disintegrates.

d. In the Field. In the event that CMS material or any other classified material is threatened with compromise due to the imminent danger of being overrun by enemy forces, all material will be burned. A stock of thermite grenades will be kept on hand for this purpose.

3. Inventory. Regardless of the emergency action or actions taken, a complete inventory of all classified material must be destroyed. This will be accomplished by using the CMS Running Inventory and the CMCC Control Log. These records must not be destroyed.

4. Reporting Emergency Action. Should the emergency destruction of classified material become necessary, the reporting of this emergency destruction is second in importance only to the actual action itself. A complete and accurate report of all CMS material destroyed, material not destroyed, and most importantly, material presumed compromised will be submitted to Commandant of the Marine Corps (CMC) (Code CCTO), Commanding General FMFPac, the Chief of Naval Operations, and the Director of the COMSEC Material System. This will be accomplished by AUTOSEVCOM or, if unavailable, an "Immediate" message (figure 4-1). For classified material not related to the COMSEC Material System, an after action report and complete inventory will be prepared and forwarded.

4002. ACTION

1. The CMS Custodian is responsible for the following requirements:

(a) Be responsible for implementation of this plan during normal working hours.

(b) Instruct CMS, communications, and security personnel and the Command Duty Officer concerning their duties in the implementation of this plan.

(c) Conduct emergency action drills at least semi-annually. The G-1 will be notified prior to a drill.

(d) Maintain training records concerning these drills for one year following the date of the drill.

2. The Command Duty Officer will meet the following requirements.

(a) Be responsible for implementation of this plan after normal working hours. Should the Command Duty Officer receive instructions to implement any part of this plan, he/she will take the information, hang-up and immediately call the authority which directed the action to verify the call. Once verified, carry out directed action.

(b) Be familiar with the contents of this order.

When instructed by the military senior conducting the destruction, send the following IMMEDIATE messages:

FROM: CG I MEF//CMS//

TO: CNO WASHINGTON DC//OP-09N//

CMC WASHINGTON DC//CTO//

DCMS WASHINGTON DC

CG FMFPAC//CMS//

UNCLAS//N02200//

SUBJ: EMERGENCY DESTRUCTION; REPORT OF A FONECON (insert the name of the individual reporting telephonic notice of emergency destruction) AND (insert names of persons receiving the calls) OF (insert the date of the telephone conversations)

A. I MEFO P5500.2

1. AS DISCUSSED DUR THE REF AN EMERGENCY DESTRUCTION HAS COMMENCED AT THIS COMMAND.

2. DETAILS OF DESTRUCTION/EXTENT OF DESTRUCTION WILL BE FWD VIA MSG ASAP.

3. CMS ACCT NR 269326.

---

*Upon completion of the destruction, send the following message:

FROM: (same as above)

TO: (same as above)

C O N F I D E N T I A L//N02200//

SUBJ: REPORT OF EMERGENCY DESTRUCTION

A. (insert date time group of previous message)

(U)1. THIS MSG AMPLIFIES THE REF.

(C)2. MATERIAL DESTROYED AS FOL:

NOMEN	ACCT NR	MEANS	CLASS	STATUS
(Note...The information contained herein is fictional and is not classified)				
KG 30	11976	PULVERIZED	CONF	N/A
USKAT 11	986	BURNED	SECRET	ROB

Figure 4-1.--Sample Message Format to Report CMS Emergency Destruction.

Checklist for Protection. In the event a determination is made to initiate procedures for increasing the security of COMSEC material, the following steps will be taken.

1. If safety conditions permit, post a guard outside of the CMS/CMCC strongroom. The guard will limit access to these areas to personnel on the appropriate access list or to personnel actively engaged in the emergency action procedures.

2. Recall personnel as indicated in figure 4-4.

3. Determine whether additional protection is warranted. Options available include the following:

    a. Arming the guard

    b. Establishing a perimeter around Building 1413

    c. Securing the area

4. Fire fighting personnel will not be prevented from approaching or entering Building 1413.

Figure 4-2.--Checklist for Protection of Classified Material.

ACCOUNTING AND TRANSMISSION OF COMMUNICATIONS
SECURITY MATERIAL SYSTEM

1. Initiating Procedures. During working hours, the command section will direct emergency removal or destruction of COMSEC material. After working hours, should the Command Duty Officer determine that COMSEC material should be removed or destroyed, the following steps will be taken:

a. Recall personnel in the sequence cited in figure 4-4.

b. If unable to contact any of the personnel cited therein, obtain the CMS vault and safe combinations from the Communications Center, Building 1133 ext. 6563.

c. On the inside of the CMS vault door are card sequences provided as guidelines for the emergency destruction of COMSEC material.

d. If the determination is made to remove COMSEC material carry out the procedures set forth in the body of this Plan.

Figure 4-3.--Checklist for Initiating Removal or Destruction of Classified Material.

ACCOUNTING AND TRANSMISSION OF COMMUNICATIONS
SECURITY MATERIAL SYSTEM

1. The sequence of personnel to be recalled in the event of any type of emergency addressed in this order are as follows:

a. The CMS Custodian (CMS Custodian and CMS Alternate Custodian(s)) home telephone numbers are provided in the recall binder at the front duty desk.

b. The Chief of Staff

c. The AC/S G-6 Operations Officer

d. The AC/S G-2 Security Manager

2. Upon the arrival of any of the above, the military senior will assume control of emergency action proceedings.

Figure 4-4.--Recall Procedures.

ACCOUNTING AND TRANSMISSION OF COMMUNICATIONS
SECURITY MATERIAL SYSTEM

PROCEDURES FOR OBTAINING COMBINATIONS TO

CLASSIFIED MATERIAL CONTAINERS

1. Attempt to contact one of the individuals listed on the wall adjacent to the CMS/CMCC strongroom (room 141).

2. In the event that none of these personnel can be located or cannot arrive in time to implement emergency action, the person who is implementing this plan will immediately proceed to the Joint Communications Center (JCC) located in the basement of the Base Headquarters (Bldg. 1169) and retrieve the combination envelopes for I MEF CMCC/CMS.

3. Once the combinations to any classified material container is signed out, the combination and all material will be considered compromised unless continuous Two Person Integrity is maintained over both the combination and the container. Therefore, it is essential that a guard be posted continuously after the combinations are signed for.

Figure 4-5.--Procedures for Obtaining Combinations to Classified Material Containers

PROCEDURES IN CASE OF A BOMB THREAT

1. In the event that there is a bomb threat called in to the I MEF Command Element, the following procedures will be used as a guide to emergency action. Safety of personnel is the prime consideration.

a. Follow the procedures outlined in figure 4-2 for emergency protection. Establish a perimeter security force only; do not station guards within the Command Element.

b. Notify the fire department and Explosive Ordnance Disposal.

c. Secure all classified material and evacuate the building. Ensure that inventories of classified materials are evacuated if possible. The CMCC inventories are located under the counter in the main office; CMS inventories are located in the top drawer of safe 14 in the strongroom.

d. Do not interfere with fire department or EOD personnel or prevent them from entering the secure area.

e. Remain clear of the building until EOD has declared it safe to re-enter.

2. In the event of an explosion, a post emergency inventory will be accomplished and any loss or unauthorized viewing of classified material will be reported to the appropriate authority.

Figure 4-6.--Procedures in Case of a Bomb Threat.

CHAPTER 5

TRAINING FOR CMS PERSONNEL

CHAPTER 5

TRAINING FOR CMS PERSONNEL

5000. GENERAL. CMS users must receive training in the handling, security, accounting, and disposition/destruction of COMSEC material they receive or use.

5001. TRAINING PROGRAM. The training required for all personnel to be designated as CMS Users will be documented and rosters will be maintained by the CMS Custodian. The CMS account Custodian must ensure this training is provided. Instructions and class outlines can be obtained from the CMS Custodian by local holders to train users of their COMSEC material.

1. Documentation. All training conducted by local holders for users of their COMSEC material will be documented (see figure 5-1). This roster will be turned in to the CMS Custodian for retention. The CMS Custodian must ensure this training is provided.

2. Topics. Specific subjects must be covered by the training program. The following are a few of the suggested topics to cover:

a. Communications Security Material System

b. Handling CMS material under Two Person Integrity

c. Reporting security violations

d. Emergency Action Plans

e. Fundamentals of routine CMS destructions

f. COMSEC material supersessions

g. Categories of COMSEC material

h. General organizational responsibility for COMSEC material

i. Storage requirements for COMSEC material

j. Protection of COMSEC material

k. Posting amendments and corrections to COMSEC manuals

l. Destruction techniques

ACCOUNTING AND TRANSMISSION OF COMMUNICATIONS
SECURITY MATERIAL SYSTEM

CMS TRAINING MUSTER

Date:

SUBJECT: _____
(BE SPECIFIC. IF MORE THAN ONE AREA IS COVERED, LIST THEM ALL)

INSTRUCTOR: _____

ATTENDEES

RATE/GRADE	NAME (PRINT)	SIGNATURE

EACH PERSON ATTENDING THIS TRAINING WILL SIGN THEIR OWN NAME ON THIS FORM

Figure 5-1. --CMS Training Muster sheet