



DEPARTMENT OF THE NAVY

COMMANDING OFFICER
NAVAL AIR STATION
700 AVENGER AVENUE
LEMOORE, CALIFORNIA 93246-5001

NASLEMINST 2280.1D CH-2
021

21 MAR 1996

NAS LEMOORE INSTRUCTION 2280.1D CHANGE TRANSMITTAL 2

From: Commanding Officer, Naval Air Station, Lemoore

Subj: HANDLING AND CONTROL OF COMMUNICATION SECURITY MATERIAL
SYSTEM (CMS)

1. Purpose. To issue pen and ink changes to basic instruction.

2. Action

a. Page 1, change Ref: (d), to read, "CMS 3A" and Ref: (e), to read, "CMS 5A."

b. Page 2, paragraph 4b(6), replace "/" with ".".

c. Page 7, paragraph 5j, second sentence, change "...Commanding Officer's permission." to read, "...written permission of the Commanding Officer, Naval Air Station Lemoore."

d. Enclosure (3), paragraph 3a(1) delete "(optional)".

e. Enclosure (5), page 4, paragraph 3d(5), add "Motorola", after "NOTE" to zeroize terminal - ".".

f. Enclosure (5), page 4, after the last line, add the following:

"Note to zeroize terminal - AT&T 1100/1150

- locate recessed zeroize button on upper right area of terminal
- use pencil/ball point pen to press
- press until button disengages"

g. Page 6, paragraph 3e(14), add "Motorola", after "NOTE" to zeroize terminal - ".".

h. Page 6, paragraph 3e(14), after line "- press red zero button..." add the following:

"NOTE to zeroize terminal - AT&T 1100/1150

- locate recessed zeroize button on upper right area of terminal

NASLEMINST 2280.1D CH-2

21 MAR 1996

- use pencil/ball point pen to press
- press until button disengages"

i. Enclosure (6), paragraph 1b, replace "concists" with "consists".

j. Enclosure (6), delete paragraphs 1c and 1d.


G. C. WOOLDRIDGE

DISTRIBUTION: (Special)
NAS Lemoore (Codes 00, 01, 10 and 021)
NAS Lemoore squadrons
STRKFIGHTWPNSCOLPAC



DEPARTMENT OF THE NAVY

NAVAL AIR STATION
LEMOORE, CALIFORNIA 93246-5001

IN REPLY REFER TO:
NASLEMINST 2280.1D CH-1
021

18 FEB 1994

NAS LEMOORE INSTRUCTION 2280.1D CHANGE TRANSMITTAL 1

From: Commanding Officer, Naval Air Station, Lemoore

Subj: HANDLING AND CONTROL OF COMMUNICATION SECURITY MATERIAL
SYSTEM (CMS)

1. Purpose. To issue "pen and ink" change to basic instruction.
2. Action
 - a. Page 1, paragraph 3, second to last line, change CMS 4, to read CMS 1.
 - b. Page 7, paragraph 5e.(4)g., last line, change CMS 4, to read CMS 1.
 - c. Enclosure 3, page 3, paragraph 6, second line, delete "CSP 1 and change CMS 4" to read CMS 1.
 - d. Enclosure 5, page 7, paragraph 4.b., last line, delete "the COMSEC Insecurities chapter" and insert "chapters 9 and 10". Change CMS 4L to read CMS 1.


A. R. GORTHY

Distribution:
CO
XO
AD
CMS
Squadrons



DEPARTMENT OF THE NAVY

NAVAL AIR STATION
LEMOORE, CALIFORNIA 93246-5001

IN REPLY REFER TO:

NASLEMINST 2280.1D

031
27 OCT 1993

NAS LEMOORE INSTRUCTION 2280.1D

From: Commanding Officer, Naval Air Station, Lemoore

Subj: HANDLING AND CONTROL OF COMMUNICATIONS SECURITY MATERIAL SYSTEM (CMS) MATERIAL

Ref: (a) OPNAVINST 5510.1H
(b) COMNAVAIRPACINST 2280.1D
(c) CMS 1
(d) CMS 3
(e) CMS 5
(f) CMS 6

Encl: (1) Statement of Responsibility for CMS Material
(2) Check List for Amendment Entry in CMS Publications
(3) Local Holder and User Responsibilities
(4) NAS Lemoore CMS Training Plan
(5) Emergency Action Plan for CMS Material
(6) End Item Accounting

1. **Purpose.** To issue control, security and distribution instructions for CMS material/STU-III's held by commands and activities who receive material from the NAS Lemoore CMS account. CMS 1 through CMS 6 are the guiding publications for CMS account management and security. This instruction amplifies those publications. Direction contained herein may be more stringent, but never more lenient than that contained in CMS 1 and other directives published by higher authority. References (a) through (f) and enclosures (1) through (6) will be used for this program.

2. **Cancellation.** NASLEMINST 2280.1C

3. **Background.** The Communications Security (COMSEC) Material System ensures accountability for distribution, handling, control and security of COMSEC materials. The CMS Custodian is the Commanding Officer's representative in all CMS matters and is directly responsible to the Commanding Officer for the accurate management and administration of the CMS account. The Custodian and alternates are appointed per the qualifications and instructions in Article 301 of CMS 4. Their guidance is binding and mandatory for local holders and responsible users.

4. **Responsibilities**

a. Commanding Officer, Naval Air Station, Lemoore, is responsible for the COMSEC material issued to the command CMS account.

27 OCT 1993

b. The CMS Custodian shall:

(1) Keep the alternate custodians informed about the current CMS management posture, files and general account status so they are always able to assume all CMS duties.

(2) Be thoroughly familiar with CMS 1 and other appropriate information sources. Obtain adequate supplies and maintain records required by CMS 1.

(3) Conduct regular training and give appropriate guidance to command personnel who are responsible for CMS material or whose duties require accurate execution of CMS procedures. Ensure the syllabus in enclosure (4) is correctly completed and documented in individual training jackets.

(4) Draw and maintain onboard the air station the required CMS material. Unless reduced holdings are authorized, hold and maintain all effective and normal reserve onboard (ROB) editions of authorized material.

(5) Issue CMS material to authorized local holders and responsible users. Ensure they have specific written instructions on storage, handling, destruction and accounting procedures.

(6) Maintain storage and physical security for CMS material per CMS 1/

(7) Ensure compliance with internal accountability safe-guards for CMS material/STU-III. In particular, monitor inventory procedures for COMSEC material at watch stations. Inventory procedures are covered in depth by Chapter 7 of CMS 1. Ensure command procedures prevent people with local custody of CMS material from detaching or departing on extended leave before turnover is completed.

(8) Page check all material to verify editions as required by CMS 1.

(9) Inform the Commanding Officer of any new or revised manuals, procedures or requirements and their effect on the account.

(10) Conduct routine destruction of CMS material, complying with authorized procedures in Chapter 5 of CMS 1 and pertinent portions of reference (a).

(11) Promptly and accurately prepare and submit CMS correspondence, messages and reports.

(12) Keep plans for emergency protection, precautionary destruction and emergency destruction of CMS material current, practical, and readily available to individuals responsible for implementing them. Emergency

27 OCT 1993

destruction will be conducted using Annex M of CMS 1, pertinent portions of reference (a) and enclosure (5).

(13) Inventory CMS material/STU-III/Key(s) as required by CMS 1.

(14) Conduct training visits with local holder accounts.

5. Specific Handling Instructions

a. Two Person Integrity. Two Person Integrity (TPI) shall be applied to classified keying material marked CRYPTO from time of receipt through destruction. At no time will a single person, regardless of grade or status be allowed access to keying material without the presence of another authorized person. Both individuals will remain with the material until all necessary transactions have been completed and the material has been secured in an approved TPI container.

(1) Only the CMS custodian and an alternate or two alternates are authorized to issue keying material to local holders and users.

(2) Two custodians/responsible users will always be present when keying material is inserted into or removed from cryptographic equipments or when extractable keying material is in use. When the keying material or loaded electronic fill device is not in use it will be afforded two person integrity by storage in approved security containers.

(3) Single person access to keying material is an incident and must be reported per Chapter 9 of CMS 1.

(4) Exception. TPI is not required when inserting key into cryptographic equipment on a flight deck or flight line. TPI must be maintained until entrance to and resumed upon exit from flight deck or flight line boundaries.

(5) STU-III. The terminal is an unclassified Controlled Cryptographic Item (CCI) when the Crypto Ignition Key (CIK) is removed and shall be protected like any other high value item. The CIK is also unclassified when removed from the terminal. The program was implemented to provide a ready available telephone for the protection of classified and sensitive information.

b. Material storage. CMS material storage must provide maximum protection against theft, compromise, loss, damage, deterioration and unauthorized access. Access by people without appropriate security clearances and the "need to know" is unauthorized. Store all CMS keying material only in approved two person integrity (TPI) containers.

27 OCT 1993

(1) CMS material not under a 24-hour watch must be stored in a GSA security container. Keymat not in use shall be kept in approved TPI locked safes until used or destroyed.

(2) Two responsible users shall inventory COMSEC material kept in a work center safe once a day or at watch change for continuously manned spaces. Forward completed inventories to the responsible custodian for retention.

(3) Change combinations to all CMS storage containers every 12 months, whenever a person who knows the combination is transferred or no longer has access to the material, or if unauthorized individuals may have gained access to the combination. Combinations to safes containing CMS keymat and cryptographic maintenance manuals shall be stored commensurate with the highest classification of the material in the safe.

(4) Arrange material in safes for ease of handling and identification for emergency destruction, segregated as follows:

- (a) TOP SECRET material.
- (b) Superseded CMS material, Secret and below.
- (c) Effective CMS material, Secret and below.
- (d) ROB material, Secret and below.

c. Watch Station Material Distribution and Handling. The Custodian and alternates will issue keymat to authorized recipients in advance of effective date to prevent communications circuit interruption.

(1) Collective Responsible User Role of Watch Station Supervisors. The individual supervisor who signs a local custody record upon receipt of keymat does so in a collective sense for all supervisors for that station. Change over of responsible user functions is an integral part of watch station supervisor relief. Local custody responsibility extends to all keymat items on the progressive listing.

(2) Progressive Listing of Keymat Held by the Watch Station. This list includes all keymat. For each item, list the short title edition suffix, accounting number, accountability legend (AL), applicable portion of segment number and related equipment short title. Add new items to the list upon receipt. As material is destroyed or entered into the destruction chain, delete it from the list, signing or initialing the change. Retain superseded progressive listing sheets for 30 days, then give them to the Custodian for destruction.

27 OCT 1993

(3) Keymat Inventory. Work center supervisors will jointly conduct a sight inventory to verify the status of all keymat held at each watch relief. Initial the appropriate column of the progressive listing to indicate keymat inventory.

(4) Keymat Page checks. CMS 1 provides comprehensive guidance on page check requirements. The following points are reiterated for emphasis.

(a) Do not page check correctly sealed primary keymat or canisters. Upon opening a previously sealed keymat package, page check the contents immediately.

(b) Page check unsealed keymat during each watch relief inventory. Use the progressive listing to determine which segments of a keymat remain accountable. If records indicate a particular keycard is in the equipment, verify it without opening the equipment only if it requires a card to function and is operating correctly.

(5) Discrepancies. Report all discrepancies to the CMS Custodian or alternates.

d. **CMS Material Destruction.** The CMS Custodian and/or alternates shall ensure all CMS material is destroyed as required, either by personally destroying the material or verifying destruction records. Material superseded daily and authorized for destruction by two responsible users shall be destroyed within 12 hours of supersession. Such material will be identified on the progressive listing and verified by the presence of a CMS 25 or locally prepared form for each keymat edition.

(1) Local Destruction Procedures. Two responsible users are required to destroy CMS material, one of whom must be the CMS Custodian or alternate.

(a) Separate the material to be destroyed from everything else similar to it. To prevent accidental destruction of unauthorized material, do not allow any material not authorized for destruction in the destruction area.

(b) Place the material to be destroyed in the same order as listed in corresponding destruction records. Verify completeness of material against local destruction records/form.

(c) Verify short titles and accounting data on the material and destruction records before inserting the material into the shredder. Never sign the destruction record before the material is actually destroyed. When a local destruction record reflects destruction of a complete accountable short title, give it to the Custodian. Follow this method to ensure success:

27 OCT 1993

1 The first person reads the short titles, accounting numbers and segment numbers to the second, who marks the date extracted and date destroyed columns of the destruction record.

2 The second person reads the short titles, accounting numbers and segment numbers to the first, who verifies the date entries on the destruction record.

3 Jointly insert the material into the shredder.

4 Insert an equal amount of similar composition paper into the shredder.

5 **BOTH SIGN THE DESTRUCTION RECORD.**

6 **JOINTLY CHECK THE RESIDUE TO VERIFY COMPLETE DESTRUCTION.**

(2) Cross-cut Shredding. Two requirements must be met to ensure complete destruction of paper COMSEC material by cross-cut shredder. If these requirements are met, the residue may be disposed of as unclassified waste.

(a) Crosscut shredders must reduce residue to shreds not more than 3/64 inch (1.2mm) wide and not more than 1/2 inch (13mm) long.

(b) When destroying small amounts of COMSEC keymat, add an equal amount of other unclassified or classified material of similar composition.

e. **Amendments**

(1) Amendments to CMS material held by responsible users and local holders will be issued to them with an SF-153 transfer document.

(2) Use enclosure (2) when entering amendments. Enter publication amendments exactly as directed by the accompanying instructions, whether making pen and ink (black) corrections, pasting in cutouts, or replacing pages. Be very cautious when replacing pages to ensure only pages authorized for removal are actually removed. Amendments which replace, add or delete pages require a careful page check of the publication, signing the Record of Page Check upon completion. After amendment entry, complete the Record of Correction page and sign and date the appropriate blanks.

(3) Page check the residue and certify correct entry using enclosure (2) to the Custodian.

(4) A second custodian/responsible user must verify correct amendment entry, initial the Record of Corrections entry, page check the publication and sign the Record of Page check, and page check the residue.

27 OCT 1993

(5) Return amendment residue to the custodian for destruction or destroy the residue as directed by the custodian and forward destruction documents to the custodian.

f. Extracts and Copies of CMS Material. Use extracts and make copies of CMS publications only with the authorization of the CMS Custodian and Commanding Officer and as approved by the controlling authority.

g. Modifications. The Custodian may recall equipment for modification or issue modifications to responsible users with an SF-153 transfer document. After entry, the responsible user will return any residue and certification of entry on an SF-153. The Custodian will destroy or any residue per CMS 4.

h. Maintenance or Repair by Crypto Repair Facility (CRF) or Maintenance Pool. If CMS equipment needs maintenance or repair beyond the capabilities of command maintenance personnel, sub-custody it to a Crypto Repair Facility (CRF) or maintenance pool of a nearby command. The repair facility is considered a temporary responsible user of the account. The person signing the SF-153 on behalf of the repair facility must be an E-6/GS-7 or above. The CMS Custodian or Alternate who turns over or picks up COMSEC equipment must present adequate identification and letter of appointment/authorization. Instructions for packaging and shipping controlled cryptographic items (CCI's) are found in CMS 1 Article 525.

i. Emergency Plan. The CMS Custodian advises the Security Manager of proper priority assignments of CMS material within the command's Emergency Plan. Post pertinent extracts from the Emergency Plan on or near all CMS material storage containers. Enclosure (5) details NAS Lemoore's Emergency Action Plan.

j. Removal of CMS Material/STU-III's. Don't remove CMS material/STU-III's from the physical confines of the command without the Commanding Officer's permission.

k. Loss or Compromise. Immediately report suspected or actual loss or compromise of CMS material to the CMS Custodian. Prepare and submit reports as required by Chapter 9 of CMS 1.

6. Statement of Responsibility. Enclosure (1) certifies to the CMS Custodian that an individual who has occasion to use CMS material has read required handling instructions and understands how to protect this material. All responsible users must have a signed statement of responsibility on file.

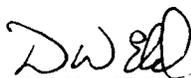
7. Action. All potential users of CMS material must familiarize themselves with CMS 1 and the applicable portions of references (a) and (b). Sign and submit enclosure (1) to the CMS Custodian to verify understanding of regulations governing handling and accountability for CMS material.

NASLEMINST 2280.1D

27 OCT 1993

8. Forms. These required forms or order information are available from the CMS Custodian.

- a. CMS Responsibility Statement.
- b. Letter of Appointment/Authorization.
- c. CMS Transfer Report (SF-153).
- d. Destruction Form (CMS-25).
- e. CMS 17 Computer Custody Card.


D. W. ELD
Acting

Distribution:

CO

XO

AD

CMS

Squadrons

27 OCT 1993

STATEMENT OF RESPONSIBILITY FOR CMS MATERIAL

From:
To: CMS Custodian, NAS Lemoore, CA
Subj: CMS RESPONSIBILITY ACKNOWLEDGEMENT
Ref: (a) NASLEMINST 2280.1D

1. I hereby acknowledge that I have read and understand reference (a).
2. I assume full responsibility for the proper handling, storage, inventorying, 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 a copy of reference (a) from the CMS custodian. If at any time I am in doubt as to the proper handling of the CMS material I am responsible for, I will immediately contact the CMS custodian and request advice.
4. Before departing on extended leave, TAD, and upon my detachment, I will check out with the CMS custodian.

Date

Signature

27 OCT 1993

CHECKOFF LIST FOR ENTERING CMS PUBLICATIONS AMENDMENTS

Amendment # _____ to _____

SIGNATURE OF PERSON ENTERING AMENDMENT: _____

- ___ 1. Amendment instructions read and understood.
- ___ 2. Prepare cutouts used when possible instead of pen and ink entries. Locally typed cutouts identify amendment number/ALCOM/DTG at bottom.
- ___ 3. Black ink used for deletions and pen and ink entries.
- ___ 4. Information superseded by cutout deleted in ink before cutout attached.
- ___ 5. Flaps used only when there's no room to attach cutout flat on page.
- ___ 6. Authority for pen and ink corrections noted in margin.
- ___ 7. Sign and date Record of Amendments page, noting amendment identification.
- ___ 8. If amendment included page replacement, page check and sign and date Record of Page Check page.
- ___ 9. If amendment included page replacement, page check amendment residue and note page check on residue. Return residue to CMS custodian for disposition.

SIGNATURE OF PERSON VERIFYING PROPER ENTRY _____

- ___ 1. Amendment instructions read and understood.
- ___ 2. Cutouts and pen and ink corrections entered correctly.
- ___ 3. Record of Amendments entry correct.
- ___ 4. Record of Page Check entry correct.
- ___ 5. If amendment replaced pages, conduct second page check, sign and date Record of Page Checks.
- ___ 6. Page check amendment residue and make page check annotation on residue.

NOTE: INITIAL EACH ITEM WHEN COMPLETED.

27 OCT 1993

(Date)

MEMORANDUM

From:

To: CMS Custodian, NAS Lemoore, CA

Subj: CERTIFICATION OF AMENDMENT ENTRY, VERIFICATION, AND LOCAL DESTRUCTION RECORD

Encl: (1) Check-off List for Entering Amendments to COMSEC Publications

1. On _____, Amendment _____, accounting number
(date) (amend number)

.RM66

_____, was entered into _____,
(serial no.) (publication short title and edition)
accounting number _____.

2. Proper entry of the amendment was verified as indicated in enclosure (1).

3. The residue of this amendment was properly destroyed on _____ by the two individuals whose signatures appear below:

(Signature)

(Signature)

(Signature of Commanding Officer)

27 OCT 1993

LOCAL HOLDER/RESPONSIBLE USER PROCEDURE

1. **Message of Appointment/Authorization.** Tenant commands and activities who hold or may need CMS material from the NAS Lemoore CMS account must formally appoint a CMS local holder custodian and alternate custodian(s) as required by CMS 1. Local holders shall send a Message of Appointment and Authorization to Draw COMSEC Material to NAS Lemoore prior to receiving COMSEC material from the NAS Lemoore account. Custodian eligibility requirements are defined in Articles 410 and 415 of CMS 1.
2. **Letter of Agreement.** A Letter of Agreement (LOA) between the local holder and NAS Lemoore is required per CMS 1. In the Letter of Agreement, the local holder command must agree to abide by and adhere to the policy and procedures in CMS 1, CMS 5, and NAS Lemoore instructions concerning proper security, control, accountability and destruction of the COMSEC material held by the local holder command. LOA's must be updated with every change of command or every three years, whichever occurs first.
3. **Records and files.** Maintain the following:
 - a. Chronological File.
 - (1) CMS running inventory (optional).
 - (2) COMSEC material reports (SF-153).
 - (3) Local inventory reports.
 - (4) Formal designation documents.
 - (5) Letter(s) of Agreement.
 - b. Correspondence and Message File.
 - (1) COMSEC material insecurity reports.
 - (2) CMS policy procedure waivers.
 - (3) Accounting correspondence and messages.
 - (4) General CMS correspondence and messages pertaining to or affecting the operation of the account.
 - c. CMS General Message File. All effective general messages (NAVOP, ALCOM, ALCOMPAC, ALCOMPAC P etc.) relating to CMS matters and affecting the account.

27 OCT 1993

d. Directives File

(1) Each effective directive of the command and higher authority in the chain of command that relates to CMS matters.

(2) Copies of messages or correspondence granting waivers of general procedures, physical security requirements or custodian/alternate custodian designation requirements, including copies of related material necessary for the full understanding of the waiver, also must be filed in the directives file until the waiver has expired or is cancelled. This requirement is in addition to the requirement to file copies of correspondence or messages involving these subjects in the correspondence and message file.

(3) If the local holder is deployed, the NAS Lemoore custodian parent account will retain copies of pertinent documents for later distribution to the local holder.

4. Sub-Custody Procedures

a. CMS Transfer Report (SF-153) will be used to transfer material to local holders and responsible users. Either form may be used for further transfer to local holder responsible users.

b. COMSEC equipment and publications issued to local holders and responsible users are accountable to the NAS Lemoore account. No permanent transfer to another is authorized. Broken equipment may be sub-custodied to a repair facility and exchanged for a temporary replacement when deployed, but the original equipment on charge to the NAS Lemoore account must be brought back upon return to NAS Lemoore.

c. While onboard NAS Lemoore, return broken equipment to the NAS Lemoore Custodian for a replacement issue.

5. Keymat distribution and control

a. Local holders may receive keymat from the CMS custodian in hardcopy or electronic form. Two local holder personnel are required to receive the keymat: The local holder custodian or alternate and another properly cleared and authorized person. Access lists must be signed by the local holder commanding officer and include the names, social security numbers and clearance certifications of the custodians, alternates and other designated individuals.

b. Local holders shall destroy superseded keymat within 12 hours of supersession and report destruction of entire editions of keymat received from NAS Lemoore not later than 72 hours after supersession.

27 OCT 1993

6. Lost Material. Local holders are responsible for reporting lost keymat or equipment per CSP 1 and CMS 4. NAS Lemoore as well as the local holder's administrative chain of command shall be info addee on all such reports.

27 OCT 1993

NAS LEMOORE TRAINING PLAN

1. **Purpose.** To issue CMS training requirements aboard NAS Lemoore.
2. **Discussion.** Everyone who handles COMSEC material needs a thorough understanding of the security and accountability requirements which guard this material and the information it protects from compromise. Each work center shall conduct regular training to keep security awareness current and at a high level.
 - a. **Required Reading.** Read the publications identified in this enclosure semiannually. Include completed required reading lists in individual training jackets and send a copy to the NAS Lemoore CMS Custodian.
 - b. **Indoctrination.** Everyone assigned to a billet requiring knowledge and handling of CMS material will check in with the CMS Custodian before assuming assigned duties.
 - c. **General Orientation.** The CMS Custodian will stress COMSEC awareness through Plan of the Day notes and monitor training in COMSEC material work centers.
3. Lesson guides and test questions are available from the CMS Custodian.
4. Incorporate CMS training into AIMD and other COMSEC user departmental training programs and maintain training documentation.

27 OCT 1993

SEMIANNUAL REQUIRED READING LIST FOR CMS USERS

MAINTENANCE PERSONNEL

OPNAVINST 5510.1H

Chapter 5
Chapter 14
Appendix F

Counterintelligence Matters
Storage
Espionage Laws

APPLICABLE KAO's

Operation Instructions

APPLICABLE KAM's

Maintenance Instructions

CMS 1

Articles 440 through 485
Chapter 5

Specific Responsibilities for CMS
Standards for Safeguarding COMSEC Material
and Information

Article 540

Article 757 and Annex Y

Chapter 9

Chapter 10

Annex M

Routine Destruction of COMSEC Material
Page Check Requirements
COMSEC Incident Reporting
Practices Dangerous to Security
Emergency Protection of COMSEC Material

NAME: _____ RATE: _____

DIV/DEPT: _____ DATE COMPLETED: _____

27 OCT 1993

SEMIANNUAL REQUIRED READING LIST FOR CMS USERS/COURIERS

OPNAVINST 5510.1H	
Chapter 5	Counterintelligence Matters
Chapter 14	Storage
Chapter 16	Courier Requirements
Appendix F	Espionage Laws
APPLICABLE KAO's	Operation Instructions
CMS 1	
Articles 440 through 485	Specific Responsibilities for CMS
Chapter 5	Standards for Safeguarding COMSEC Material and Information
Article 540	Routine Destruction of COMSEC Material
Chapter 9	COMSEC Incident Reporting
Chapter 10	Practices Dangerous to Security
Annex M	Emergency Protection of COMSEC Material
Article 260	Routine Destruction of COMSEC Material
Chapter 3	Emergency Protection of COMSEC Material

NAME: _____ RATE: _____

DIV/DEPT: _____ DATE COMPLETED: _____

27 OCT 1993

SEMIANNUAL REQUIRED READING LIST FOR CMS USERS

OPNAVINST 5510.1H

Chapter 5
Chapter 14
Chapter 15
Appendix F

Counterintelligence Matters
Storage
Transmission
Espionage Laws

APPLICABLE KAO's

Operation Instructions

CMS 1

Articles 440 through 485
Chapter 5

Specific Responsibilities for CMS
Standards for Safeguarding COMSEC Material
and Information

Article 540

Routine Destruction of COMSEC Material

Article 757 and Annex Y

Page Check Requirements

Chapter 9

COMSEC Incident Reporting

Chapter 10

Practices Dangerous to Security

Annex M

Emergency Protection of COMSEC Material

NAME: _____ RATE: _____

DIV/DEPT: _____ DATE COMPLETED: _____

27 OCT 1993

SEMIANNUAL REQUIRED READING LIST FOR CMS CUSTODIANS/ALTERNATES

OPNAVINST 5510.H	
Chapter 2	Program Management
Chapter 5	Counterintelligence Matters
Chapter 14	Storage
Chapter 15	Transmission
Chapter 16	Courier Requirements
Appendix F	Espionage Laws
APPLICABLE KAO's	Operation Instruction
APPLICABLE KAM's	System Security
CMS 1	
Articles 410 through 485	Selection and Responsibilities for CMS Personnel
Chapter 5	Standards for Safeguarding COMSEC Material and Information
Article 540	Routine Destruction of COMSEC Material
Articles 703 through 715	Control and Documentation Requirements for COMSEC Material
757, 763 and 787	
Chapter 9	COMSEC Incident Reporting
Chapter 10	Practices Dangerous to Security
Annex M	Emergency Protection of COMSEC Material

NAME: _____ RATE: _____

DIV/DEPT: _____ DATE COMPLETED: _____

27 OCT 1993

**NAS LEMOORE EMERGENCY ACTION PLAN
FOR COMMUNICATIONS SECURITY (CMS) MATERIAL**

Ref: (a) CMS 1
(b) CMS 6
(c) OPNAVINST 5510.1H

1. **Purpose.** To issue the NAS Lemoore Emergency Action Plan for COMSEC material/STU-III's following reference (a) through (c).

2. **Discussion.** Unauthorized access to classified cryptographic information must be prevented. In an emergency involving danger to or capture of classified material, it's critically important to protect this information by removal, partial or complete destruction. Two person integrity (TPI) procedures will be observed whenever practicable. If two custodian/responsible users are not available use two personnel with appropriate clearances. Second only to this protection is keeping an inventory and reporting what material was actually destroyed.

a. **Personnel safety must be emphasized.** The senior person present at work centers effecting emergency removal or destruction is responsible for taking all possible measures to prevent injury or death of participating personnel. Do not endanger personnel to protect CMS material.

b. Two categories of emergencies exist; accidental and hostile action. Accidental emergencies include natural disasters (earthquakes) and operational casualties (fire, aircraft crash). Hostile action emergencies include terrorist action, enemy attack and mob action.

3. **Action.** Implement part or all of this plan only when directed by competent authority: The Commanding Officer, Executive Officer, CMS Custodian or alternates, or the senior officer or petty officer present. While not every conceivable situation is covered in this instruction, use of these guidelines and consultation with the CMS Custodian will allow successful problem resolution.

a. **Accidental Emergencies**

(1) Fire. **Personnel safety is of primary importance.** Take action to put out a fire only when it's minor, easily contained and not life endangering. When in doubt, clear the area and let the fire department handle it.

27 OCT 1993

NOTE: Remember! TPI is in effect.

(a) Report the fire (extension 911). Notify CMS Custodian or alternates. If practical, the senior person present will take custody of the running inventory, local destruction records and inventory documents.

(b) Secure as much CMS material as possible. Admit fire fighters without delay. The CMS Custodian, alternates or on-scene leader will keep track of CMS material location as much as possible. When the fire is out and the area secured, obtain the names of all fire fighters granted access to restricted spaces.

(c) Inventory CMS material/STU-III's and make any required reports. The CMS Custodian will keep the Commanding and Executive Officers fully informed.

(2) Earthquake. Most earthquakes in this area aren't strong enough to damage space integrity. Take the following action in the event an earthquake of sufficient magnitude occurs:

NOTE: Remember! TPI is in effect.

(a) Secure all COMSEC material/STU-III's in appropriate containers. Post guards by space entry points to prevent unauthorized access.

(b) Immediately notify the CMS Custodian or alternates. If directed, the senior person present will take custody of the running inventory, local destruction and inventory documents.

(c) Admit emergency relief personnel to spaces as required without delay. As with fire procedures, the Custodian or senior person present will note names of all personnel admitted to restricted spaces.

(d) Inventory all COMSEC material/STU-III/key(s) as soon as spaces are safely accessible and make required reports. The CMS Custodian will keep the Commanding and Executive Officers fully informed.

(3) Aircraft Crash. Handle the results of an aircraft crash in or near spaces containing COMSEC material in the same general manner as for fire or earthquake. The squadron local holder custodian will submit Lost Material Reports per reference (b) for COMSEC equipment onboard the aircraft and lost in the crash.

b. Hostile Action Emergencies. Three threat levels comprise hostile action emergencies. Once competent authority has determined the threat level, take the following action, observing TPI procedures when practicable/applicable:

27 OCT 1993

NOTE: Notification will be verbally passed by Commanding Officer/CDO to department heads.

(1) Threat Stage One: Potential Emergencies. Hostile activity indicates the command is in a high-risk environment. Advance warning may be three months to within three days of predicted incident occurrence.

NOTE: Remember! TPI is in effect.

(a) Reduce Account Holdings. Responsible users with COMSEC material/STU-III/key(s) will return it to the CMS Custodian. Local holder command COMSEC emergency action plans will be implemented and the results reported to the NAS Lemoore CMS Custodian.

(b) During threat stage one, the authorized reduction procedures are, in descending order of desirability:

- Transfer material to an account in a lower risk environment.
- Remove material by sub-custody to a location in a lower risk environment.
- Partial precautionary destruction.

(2) Threat Stage Two: Probable Emergency. Terrorist activity, mob action or international tensions make COMSEC material compromise by hostile action likely. Advance warning may be within one to three days of predicted incident occurrence. Conduct partial precautionary destruction.

(3) Threat Stage Three: Imminent Emergency. Terrorist activity, mob action or enemy attack makes CMS material compromise by hostile action inevitable. No advance warning is possible. The time available to complete necessary actions will be dictated by events. **PERSONNEL SAFETY MUST REMAIN A PRIORITY.** Conduct complete destruction of COMSEC material.

c. Partial Precautionary Destruction. Destroy all material not essential to current operations. The primary value of this action is that if an overrun threat becomes imminent, total destruction can be completed relatively quickly. Note what material you destroy on the running inventory and destroy material in this order:

(1) Superseded Keying material:

- Top Secret, primary keymat.
- Secret, Confidential and unclassified primary keymat.

27 OCT 1993

(2) Reserve on board (ROB) keymat for use more than a month in the future.

(3) Non-essential classified manuals: (remove sensitive pages first)

- Maintenance manuals (KAM)
- Operating manuals (KAO)
- Administrative manuals (CMS)

d. Complete emergency destruction following partial precautionary destruction. Destroy the remaining material in this order:

(1) Effective Keying Material:

- Top Secret primary keymat
- Secret, Confidential and unclassified primary keymat.

(2) Essential classified COMSEC manuals

(3) COMSEC equipment

(4) All remaining COMSEC related material

(5) STU-III's

- Zeroize operational keying material - top secret, secret, confidential, unclassified.

- Zeroize seed keying material - top secret, secret, confidential, unclassified.

- Zeroize all loaded STU-IIIs - top secret, secret, confidential, unclassified.

"NOTE" to zeroize terminal -

- locate access door on upper left area of terminal.
- open access door.
- press red zero button until it disengages from detent and release button.

27 JUN 1993

- if capture is imminent and key has not been zeroized, remove key, separate ID tag and key, and discard key and ID tag in a widely separated area.

- If lack of power prohibits keying material (fill device) or a loaded terminal from being zeroized, ensure that all keying material and CIK's are physically removed from the area. In extreme emergencies, an attempt to physically destroy fill devices and CIKs is allowed. Material can be burned or broken as much as possible to prevent unauthorized use.

e. Complete Emergency Destruction with no Prior Warning. Note what material you destroy on the running inventory and destroy material in this order:

(1) All superseded keymat designated CRYPTO, and Secret and Top Secret tactical operations codes and authentication systems.

(2) Effective keymat designated CRYPTO (including keying variables stored electrically in crypto equipment), except ROB two-holder keymat and ROB one-time pads.

(3) Superseded Confidential and unclassified tactical operations codes.

(4) ROB Top Secret multiholder keymat designated CRYPTO which will become effective within the next 30 days.

(5) ROB Secret and Confidential multiholder keymat designated CRYPTO which will become effective within the next 30 days.

(6) All remaining classified keymat, authentication systems, maintenance and sample keymat, ROB two-holder keymat, and ROB one-time pads.

(7) Complete crypto maintenance manuals or their sensitive pages.

(8) Status documents showing the effective dates for COMSEC keymat (CSPM 3).

(9) Keymat holder lists and directories (CMS 32).

(10) Remaining classified pages of crypto maintenance manuals.

(11) Crypto operating instructions (KAO).

(12) Remaining classified COMSEC documents.

27 OCT 1993

(13) COMSEC equipment.

- Zeroize the equipment.
- Remove and destroy readily removable classified elements (printed circuit boards).
- Destroy remaining classified elements. Once all classified elements are destroyed, it's not necessary to further destroy the equipment.

(14) STU-III's

- Zeroize operational keying material - top secret, secret, confidential, unclassified.
- Zeroize seed keying material - top secret, secret, confidential, unclassified.
- Zeroize all loaded STU-IIIs - top secret, secret, confidential, unclassified.

"NOTE" to zeroize terminal -

- locate access door on upper left area of terminal.
- open access door.
- press red zero button until it disengages from detent and release button.
- If capture is imminent and key has not been zeroized, remove key, separate ID tag and key, and discard key and ID tag in a widely separated area.
- If lack of power prohibits keying material (fill device) or a loaded terminal from being zeroized, ensure that all keying material and CIK's are physically removed from the area. In extreme emergencies, an attempt to physically destroy fill devices and CIKs is allowed. Material can be burned or broken as much as possible to prevent unauthorized use.

4. Reporting Emergency Destruction

- a. The senior official shall report facts surrounding the destruction to Chief of Naval Operations (CNO), Director COMSEC Management Security (DCMS), Director of National Security Agency (DIRNSA), and both operational and

27 OCT 1993

administrative command echelons as soon as possible; if feasible, use a secure means of reporting.

b. State in the report the material destroyed by, short title, serial number, method and extent of destruction, and any classified COMSEC material items presumed to have been compromised (e.g., items either not destroyed or not completely destroyed). If feasible, follow the reporting procedures outlined in the COMSEC Insecurities chapter of the CMS 4L.

(1) Submit INITIAL COMSEC INCIDENT REPORT PER CMS 1, CHAPTER 9. Refer to EXAMPLE:

EXAMPLE

ADMINISTRATIVE MESSAGE

IMMEDIATE

DATE TIME GROUP (DTG)

FM NAS LEMOORE CA//021//

TO DIRNSA FT GEORGE G MEADE MD//X71A//
 CINCPACFLT PEARL HARBOR HI//JJJ//
 NAVELEXSECCEN WASHINGTON DC//JJJ//
 UCCINCPAC HONOLULU HI//JJJ//
 USSPACECOM PATERSON AFB CO//JJJ//
 DCMS WASHINGTON DC//DCMS//
 NAS FALLON NV//JJJ//

INFO: COMNAVCOMTELCOM WASHINGTON DC//N32/N3/NX//
 DCMS WASHINGTON DC//T20//
 (If LOSS or COMPROMISE: INFO: CNO WASHINGTON DC/N652//
 COMNISCOM WASHINGTON DC)

BT

SECRET//N02280// (CLASSIFICATION OF HIGHEST MATERIAL INVOLVED)
 MSGID/GENADMIN/NAS LEMOORE CA//
 SUBJ/INITIAL REPORT OF COMSEC INCIDENT//
 RMKS/

1. CMS account number 251090
2. Identify material involved. Include: (For keying material, coded manuals, and repair manuals) Full short titles and edition; Accounting number; Segments, tables, and pages, if not a complete edition or document; and the classification.

27 OCT 1993

(For equipment) Nomenclature of system designator; modification number(s) if applicable; serial number of AL1 equipment (All others by quantity); and associated or host equipment. If the equipment was keyed, also identify the information previously identified for keying material.

3. Identify the personnel involved. Provide duty position and level of security clearance.

4. Describe the circumstances surrounding the incident. Give chronological account. Give a clear picture of how the incident occurred. For example: Date, time, fire was discovered in building... or earthquake damaged building... or hostile action forced emergency destruction action to be taken by order of Commanding Officer... etc...

5. Provide command's estimate of possibility of compromise with one of the following opinions:

COMPROMISE: The material was irretrievably lost or available information clearly proves that the material was made available to an unauthorized person or persons.

COMPROMISE NOT TO BE RULED OUT: Available information indicates that the material could have been made available to an unauthorized person, but there is no clear proof that it was made available.

NO COMPROMISE: Available information clearly proves that the material was not made available to an unauthorized person.

"NOTE"

During actual hostilities, loss of keying material must be immediately reported to each controlling authority by the most expeditious means available so that supersession or recovery action can be taken.

6. Include additional information: Known or suspected sabotage, capture, or hostile activity. Describe the individuals knowledge of COMSEC, cryptoprinciples, and protective technologies. If intact CMS material is lost or captured, describe the circumstances of last sighting; provide any available information concerning the cause of the disappearance. Describe the action taken to locate the material. Estimate the possibility that material may have been removed by authorized or unauthorized persons. Describe the methods of disposal of classified and unclassified material and the possibility of loss by those methods.

7. State whether an investigation has been initiated. If so, identify the type of investigation initiated (e.g., local command inquiry, NIS, JAG, etc.).

8. Indicate whether an SF-153 lost or found material accounting report will be forwarded. If so, identify transaction number, if known. If in EMERGENCY ACTION, N/A will apply.

9. Include the name and telephone number of an individual who is prepared to respond to questions from the evaluating authority.

27 OCT 1993

END ITEM ACCOUNTING

1. End item accounting procedures allow for separately accountable ancillary components, held in conjunction with basic COMSEC equipment, to be accounted for as a single Short Title, as follows:

a. The KYK-13-01 configuration consists of the KYK-13 and ancillary cable, and will be inventoried same.

b. The KOI-18-1 configuration consists of the KOI-18 and ancillary cable, and will be inventoried same.

c. The KIR-1A-1 configuration consists of the KIR-1A and Z-ACA power supply, and will be inventoried same.

d. The KIT-1A-1 configuration consists of the KIT-1A and the Z-ACA power supply, and will be inventoried same.

2. All cryptographic equipment must be handled and accounted for as a complete equipment configuration except when only the basic unit is held.