



DEPARTMENT OF THE NAVY

NAVAL WEAPONS STATION YORKTOWN
P.O. DRAWER 160
YORKTOWN, VA 23691-0160

WPNSTA YORKTOWNINST 2281.2
EKMS Custodian
28 Nov 01

NAVAL WEAPONS STATION YORKTOWN INSTRUCTION 2281.2

Subj: PROCEDURES FOR INTERNAL DISTRIBUTION AND CONTROL OF COMMUNICATIONS SECURITY (COMSEC) MATERIAL AND SECURE (STU-III) TELEPHONES

Ref: (a) CMS 21A
(b) CMS 6
(c) EKMS-702.01 STU-III Key Management Plan

Encl: (1) CMS Material Support Letter of Agreement
(2) CMS Responsibility Acknowledgment Form
(3) STU-III Letter of Appointment and Acknowledgment Form
(4) Local COMSEC Destruct Form (CMS-25)

1. Purpose. To issue local procedures for the distribution, use, and control of COMSEC (CMS) material and STU-III telephones for WPNSTA Yorktown and all tenant commands and storefronts serviced.

2. Cancellation. WPNSTA YORKTOWN INSTRUCTION 2281.1

3. Background. CMS provides for the security of certain highly sensitive classified material and related software and hardware. Because of the nature and sensitivity of CMS material, positive accountability for the material is needed from the time of its entry into the system until it is destroyed or transferred from the system. Detailed instructions for issuing, accounting, handling, safeguarding, destroying, and disposing of CMS material, including STU-III telephones (and keys), are outlined in references (a) through (c). Chapter One of this instruction provides local guidance concerning CMS material, Chapter Two provides similar guidance related to STU-III telephones and keys.



K. L. SKUDIN

Distribution:

Navy Regional Security Directorate, Peninsula Precinct
Regional Port Ops Program, Yorktown Site
EODMU TWO Det
NAGE, LOCAL R4-1
BRMEDCLINIC Yorktown
NSWCIHDIV DET Yorktown, Code 70
NSWCIHDIV DET Yorktown, Code 930
LANTORDCOM Yorktown
NAVAIRWARCENWPNSDIV DET Yorktown
NAVOPTHALSUPTRACT Yorktown
NAVSEA DET RASO Yorktown
SECFASTCO Yorktown
FISC Cheatham Annex
FLTHOSUPPOFF DET Williamsburg
NAVCHAPGRU Williamsburg
NAVSEAMATREP Williamsburg

28 NOV 2001

CHAPTER ONE
CMS MATERIAL

1. Responsibilities

a. EKMS Custodian. Per reference (a), the Commanding Officer (CO) will appoint a EKMS Custodian in writing. The EKMS Custodian is responsible to the CO for the proper administration of the Command's CMS Account. The custodian also serves as the principal advisor to the CO on matters concerning the proper handling of COMSEC material, records, and reports. The duties and responsibilities of the EKMS Custodian are outlined in reference (a).

b. Alternate EKMS Custodian. The CO will also appoint alternate EKMS Custodians in writing. The alternate custodians help the EKMS Custodian with CMS-related duties. The duties and responsibilities of the Alternate EKMS Custodian are outlined in reference (a).

c. CMS User. A person having the proper security clearance and "need-to-know" to accept responsibility of COMSEC material from the EKMS Custodian, or another CMS User, by signing a local custody document as a CMS User. CMS Users shall follow the security, control, and internal accountability procedures of reference (a), this instruction, and any additional technical and managerial guidance given by the EKMS Custodian. In those instances where a CMS User is responsible to a Commanding Officer other than that of the numbered CMS account command, a COMSEC Material Support Letter of Agreement, enclosure (1), must be executed between the CMS account command and the User command.

d. EKMS Witness. Any properly cleared U.S. Government employee (military or civilian) who may be called upon to assist a Manager or Local Element in performing routine administrative tasks related to the handling of COMSEC material. A witness must carry the proper clearance and must be authorized access to keying material in writing by the Commanding Officer.

e. EKMS Management. The EKMS Custodian is not exclusively responsible for the management and security of COMSEC material. Management and security of COMSEC material are inherent responsibilities at all levels of command. Proper evaluation of CMS administrative procedures can only be made by those individuals in the chain-of-command who understand CMS requirements. It is necessary that officers senior to the EKMS Custodian in the operational chain-of-command (i.e., CO/XO) familiarize themselves with the management and security requirements of COMSEC material.

2. Procedures

a. Classification. The classification of COMSEC material is indicated by the standard classification markings: Top Secret (TS), Secret (S), Confidential (C), or Unclassified (U). The security classification assigned to COMSEC material determines its storage and access requirements as directed by OPNAVINST 5510.1 (series). The marking or designation "CRYPTO" identifies all COMSEC keying material used to protect or authenticate classified or sensitive unclassified information, the loss of which could adversely affect national security. The marking "CRYPTO" is not a security classification.

28 NOV 2001

b. Access. Only those persons who have a "need-to-know" and possess the proper security clearance shall be granted access to COMSEC material. Also, each CMS User must complete a CMS Responsibility Acknowledgment Form, enclosure (2), certifying that they have read and thoroughly understand all applicable provisions of reference (a) and this instruction.

c. Two-person Integrity (TPI). TPI is a system of handling and storing to prevent single-person access to certain COMSEC material.

(1) TPI handling requires that at least two persons, authorized access to COMSEC keying TPI material, be in constant view of each other and the material requiring TPI whenever that material is accessed and handled.

(2) TPI storage requires the use of at least two approved combination locks (each with a different combination) with no one person authorized access to containers.

d. Transfer of Material. All transactions concerning the receipt, return, transfer, issue or destruction of COMSEC material will be effected via a Standard Form 153 prepared by the EKMS Custodian.

e. Removal of COMSEC Material. Under no circumstances will COMSEC material be removed from this Station by anyone other than the EKMS Custodian/Alternate.

3. Storage

a. Spaces. Storage spaces for COMSEC material shall give maximum protection against unauthorized personnel access and material damage or deterioration. Storage spaces shall be secured when not under the direct supervision of properly cleared and authorized personnel. Storage containers for COMSEC material outside the CMS vault shall be approved by the EKMS Custodian and will meet the requirements of Annex N of reference (a).

b. Combinations. Knowledge of the combination(s) to the EKMS Custodian vaults and safes shall be limited to the custodian and alternate custodians. Combinations of containers used to store COMSEC material held by CMS Users shall be limited to personnel with "need -to-know" and proper clearance. A record of combinations shall be kept as directed by Chapter 5 of reference (a).

c. Posting. The following information shall be posted on each security container or vault used to store COMSEC material:

"IF THIS CONTAINER IS FOUND OPEN:

- POST A GUARD
- CONTACT THE CDO AND SECURITY DISPATCHER
- RECALL INDIVIDUALS RESPONSIBLE FOR CONTAINER
- DO NOT TOUCH CONTAINER OR ITS CONTENTS"

4. Reproduction. COMSEC material may only be reproduced by the EKMS Custodian or Alternate.

5. Damaged/Worn/Mutilated CMS Publications. Any such publications will be returned to the EKMS Custodian or Alternate.

28 NOV 2001

6. Amendments/Changes/Corrections. All amendments, changes or corrections will be entered by the EKMS Custodian or Alternate.

7. Destruction Procedures. The EKMS Custodian/Alternate, CMS User, or a properly cleared witness shall destroy COMSEC keying material as follows:

a. COMSEC material to be destroyed will be separated and removed from the general area from all other similar material being retained.

b. The COMSEC material to be destroyed will be arranged in the same order as it appears on the local destruction record.

c. The person responsible for conducting the destruction shall read the short title, edition, accounting numbers, and card numbers to the witness who will mark the appropriate entries on the destruction record. Conduct page checks of paper documents with care ensuring pages are not stuck together.

d. In turn, the witness shall read the short titles, edition, accounting numbers, and card numbers to the person responsible for conducting the destruction who will mark the appropriate entries on the destruction record. Conduct page checks of paper documents with care ensuring pages are not stuck together.

e. Immediately after verifying the accuracy and completeness of the line entries, one person will insert the material into the shredder/destroy material, while the other person witnesses the destruction.

8. Security Violations

Any actual or suspected loss or compromise of COMSEC material shall be reported immediately to the EKMS Custodian. The EKMS Custodian shall then notify the CO and take appropriate actions as outlined in reference (a).

9. Emergency Action Plan. The EKMS Custodian shall make sure that a detailed plan for emergency destruction of COMSEC material is prepared and updated periodically. All CMS Users will thoroughly familiarize themselves with the provisions in the Emergency Action Plan, and destroy COMSEC material accordingly should such an order be issued.

10. Training. The EKMS Custodian shall ensure that CMS Users and CMS administrative personnel fully understand their CMS responsibilities and are sufficiently trained to carry out those duties.

28 NOV 2001

CHAPTER TWO
SECURE (STU-III) TELEPHONES

1. Responsibilities

a. STU-III COMSEC Account (SCA) Custodian. The SCA Custodian and SCA Alternate at WPNSTA Yorktown are the appointed EKMS Custodian and Alternate EKMS Custodian. The SCA Custodian and alternate are responsible for the proper administration, handling of material, required records and reports as outlined in references (b) and (c), and this instruction.

b. Custody Signature Responsibility (CSR) Representative. The CSR representative is a person, appointed in writing by the CO, OIC, or department head, that has proper security clearance and "need-to-know" to accept custody of STU-III SCA material from the SCA Custodian.

(1) The CSR representative is responsible for posting a list of authorized STU-III account users in the immediate area of STU-III terminals under their cognizance.

(2) The CSR representative shall be appointed using enclosure (3).

c. STU-III Account User. An account user is a properly cleared and authorized person who requires STU-III material to accomplish an assigned duty.

(1) An account user may obtain required materials from the SCA Custodian or through the designated command Custody Signature Responsibility (CSR) representative.

(2) Account users are responsible for the proper security, control, accountability, and disposition of material placed in their charge complying with applicable requirements of references (b) and (c), and this instruction.

(3) Account users will be designated utilizing enclosure (3).

2. Procedures

a. Access. Only properly designated STU-III account users shall be granted access to Cryptographic Ignition Keys (CIKs) or STU-III terminals with CIKs inserted. Only persons designated on the STU-III Letter of Appointment and Acknowledgment Form, enclosure (3), will be allowed access.

b. Transfer of Material. All transactions concerning the issue or return of SCA material will be effected by the SCA Custodian on an SF-153 Form.

c. Accountability. STU-III terminals and keys will be inventoried, and records maintained, by the SCA Custodian in accordance with requirements established in references (a) and (b).

d. Insecure Practices. Unless there is an indication of espionage or sabotage, insecure practices are not reportable outside the command. The COMSEC account command will monitor and evaluate insecure practices for possible action.

28 NOV 2001

(1) STU-III account users must report any insecure practices immediately to the SCA Custodian.

(2) Do not transmit classified information using a terminal whose display has failed.

(3) Following is a list of some *reportable* insecure practices:

(a) Authentication information in terminal display is not representative of the organization (distant of local terminal).

(b) Any display indicating compromise.

(c) Any instance where there is a loss of material, material is left unattended, improperly stored, or improperly destroyed.

e. Security of STU-III Equipment

(1) When the CIK is removed, the STU-III terminal is unclassified.

(2) STU-III terminals will not be operated at a level higher than classification level indicated on the terminal display.

(3) CIKs associated with STU-IIIs will be protected to the level of the applicable keyed terminal.

(4) CIKs will not be removed from the Station.

(5) It is the responsibility of STU-III users to make sure that classified conversations are not overheard by those who do not have the proper clearance or "need-to-know."

(6) Transmission of classified data via STU-III terminals using computer or FAX must be approved in writing by the Command authority for each individual system. This written authorization must be renewed annually.

28 NOV 2001

From: Commanding Officer, Naval Weapons Station Yorktown
To:

Subj: COMSEC MATERIAL SUPPORT LETTER OF AGREEMENT

Ref: (a) CMS-21a
(b) CMS-6
(c) WPNSTA YORKTOWNINST 2281.2

1. WPNSTA Yorktown agrees to provide COMSEC material/STU-III support to your command with the following provisions:

a. Compliance with References. Commanding Officer, _____ will ensure that all personnel authorized to handle and use COMSEC materials provided by WPNSTA Yorktown comply with the guidance of references (a) through (c). To this end, _____ will conduct training at regular intervals on the proper handling, accounting, use and safeguarding of COMSEC material. Particular emphasis must be given to educating personnel in how to identify COMSEC incidents and practices dangerous to security (PDS).

b. Responsibility for Certifying Clearances/Access. Commanding Officer, _____ accepts full responsibility for ensuring that all personnel whose duties require them to use COMSEC materials are properly cleared and formally authorized access to COMSEC material. You are also required to have personnel complete a CMS Responsibility Acknowledgement Form/STU-III Letter of Appointment and Acknowledgement Form enclosures (2) and (3) (as applicable), and forward a copy to WPNSTA Yorktown EKMS Custodian, prior to being issued COMSEC material.

c. Access to Keying and PAL COMSEC Material. Commanding Officer, _____ will designate, in writing, all personnel authorized access to COMSEC keying material (KEYMAT) and PAL material/teams. Provide a copy of this in writing to WPNSTA Yorktown EKMS Custodian.

d. Safe/Vault Certification. Commanding Officer, _____ will provide WPNSTA Yorktown EKMS Custodian written certification of all safes and/or vaults used to store COMSEC material.

e. Reporting of COMSEC Incidents. In the event of a COMSEC incident, Commanding Officer, _____ will immediately report such incident to WPNSTA Yorktown EKMS Custodian and provide all necessary support in investigation of reported incident.

Proposed:

Concur:

Commanding Officer
Naval Weapons Station Yorktown

Commanding Officer

28 NOV 2001

CMS RESPONSIBILITY ACKNOWLEDGEMENT FORM

From: _____ (Full Name) _____ (Rank/Rate)
_____ (Social Security Number) _____ (Command)

To: EKMS Custodian, Naval Weapons Station Yorktown

Subj: CMS RESPONSIBILITY ACKNOWLEDGMENT FORM

Ref: (a) WPNSTA YORKTOWNINST 2281.2

1. I hereby acknowledge that I have read and fully understand reference (a).
2. I assume full responsibility for the proper handling, storage, accounting, transfer, and disposition of COMSEC material held in my custody and/or used by me.
3. I have received instructions on the handling of COMSEC material from the EKMS Custodian. If at any time I am in doubt as to the proper handling or status of COMSEC material, I will immediately contact the EKMS Custodian.
4. Before I depart on any extended departure (in excess of 30 days), or detachment, I will check out with the WPNSTA Yorktown EKMS Custodian and be relieved of any COMSEC material I have signed for.

Signature: _____ Date: _____

STU-III LETTER OF APPOINTMENT AND ACKNOWLEDGEMENT FORM

From: _____
(CO/OIC/Department Head) (Command/Department)

To: STU-III COMSEC Account (SCA) Custodian, Naval Weapons Station Yorktown

Subj: ASSIGNMENT OF STU-III USER PERSONNEL

Ref: (a) WPNSTA YORKTOWNINST 2281.2

1. The following personnel of this command/department are designated as follows:

a. Custody Signature Responsibility (CSR) Representative:

(Name) (Rank) (SSN) (Signature)

b. Designated STU-III Account Users:

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

(2) I assume full responsibility for the safe handling, storage, accounting, and transfer of SCA material held in my custody and/or used by me.

(3) I have received instruction on the handling of SCA material. If at any time I am in doubt as to proper handling or status of SCA material, I will immediately contact the EKMS Custodian.

<u>NAME</u>	<u>RANK</u>	<u>SSN</u>	<u>SIGNATURE</u>
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Signature: _____
(CO/OIC/Department Head)

28 NOV 2001

CONFIDENTIAL (When Filled In)

LOCAL COMSEC DESTRUCT FORM (CMS-25)
(One-time Keying Material)

Retain form locally for 90 days.

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

No.	Date Extracted	Date Destroyed	Signature	Signature
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				

Short Title: _____ Edition: _____

Formal destruction of entire publication in accordance with CMS 21A:

TN: _____ / _____ Dated: _____

Grade/Signature: _____ Grade/Signature: _____

CLASSIFIED BY CMS-21A

CONFIDENTIAL (When Filled In)