DIRECTOR,
COMMUNICATIONS SECURITY MATERIAL SYSTEM
3801 NEBRASKA AVE, NW
WASHINGTON DC 20393-5453

CMS 1

COMMUNICATIONS SECURITY MATERIAL SYSTEM (CMS) POLICY AND PROCEDURES MANUAL

ORIGINAL
(REVERSE BLANK)

LIST OF EFFECTIVE PAGES

PAGE NUMBERS	EFFECTIVE PAGES
FRONT COVER (REVERSE BLANK)(UNNUMBERED)	ORIGINAL
I (REVERSE BLANK)	ORIGINAL
III, IV	AMEND 4
IV.I (REVERSE BLANK)	AMEND 4
V (REVERSE BLANK)	AMEND 4
VI (REVERSE BLANK	AMEND 4
IX thru XXX	AMEND 4
1-1 thru 106	AMEND 4
2-1 thru 2-11 (REVERSE BLANK)	AMEND 4
3-1 thru 3-7 (REVERSE BLANK)	AMEND 4
4-1 thru 4-2	AMEND 4
4-3, 4-4	ORIGINAL
4-5, 4-6	AMEND 1
4-7 thru 4-10	AMEND 4
4-10.1 (REVERSE BLANK)	AMEND 4
4-11, 4-12	AMEND 1
4-13 thru 4-18	ORIGINAL
5-1 thru 5-10	ORIGINAL
5-11 thru 5-14	AMEND 1
5-15 thru 5-22	ORIGINAL
5-23 thru 5-25	AMEND 1
5-26 thru 5-28	ORIGINAL
5-29 thru 5-51 (REVERSE BLANK)	AMEND 4
6-1, 6-2	AMEND 4
6-3, 6-4	AMEND 1
6-5	AMEND 4
6-6 thru 6-8	AMEND 1
6-8.1 (REVERSE BLANK)	AMEND 1
6-9 thru 6-17 (REVERSE BLANK)	AMEND 4
7-1 thru 7-6	ORIGINAL
7-7 thru 7-10	AMEND 4
7-10.1 (REVERSE BLANK)	AMEND 4
7-11, 7-12	ORIGINAL
7-13 thru 7-16	AMEND 4
7-16.1 (REVERSE BLANK)	AMEND 4
7-17, 7-18	AMEND 1
7-19, 7-20	ORIGINAL
7-21 (REVERSE BLANK)	AMEND 3
7-22 thru 7-24	AMEND 3
7-24.1 (REVERSE BLANK)	AMEND 3
7-25 thru 7-29	AMEND 4
7-29.1	AMEND 4
7-29.2	AMEND 3
7-30	AMEND 3

LIST OF EFFECTIVE PAGES

PAGE NUMBERS	EFFECTIVE PAGES
7-31, 7-32	AMEND 4
7-32.1 (REVERSE BLANK)	AMEND 4
7-33, 7-34	ORIGINAL
7-35, 7-36	AMEND 1
7-37, 7-38	ORIGINAL
7-38.1 (REVERSE BLANK)	ORIGINAL
7-39 thru 7-42	AMEND 4
7-42.1 (REVERSE BLANK)	AMEND 4
7-43 thru 7-52	ORIGINAL
7-53, 7-54	ORIGINAL
7-55 (REVERSE BLANK)	ORIGINAL
7-57 thru 7-59 (REVERSE BLANK)	ORIGINAL
7-61 thru 7-65 (REVERSE BLANK)	ORIGINAL
8-1, 8-2	AMEND 1
8-2.1 (REVERSE BLANK)	AMEND 1
8-3 thru 8-6	AMEND 4
9-1 thru 9-4	ORIGINAL
9-5, 9-6	AMEND 4
9-6.1 (REVERSE BLANK)	AMEND 4
9-7 thru 9-14	ORIGINAL
9-14.1 (REVERSE BLANK)	ORIGINAL
9-15, 9-16	AMEND 1
9-17 thru 9-20	AMEND 4
9-20.1, 9-20.2	AMEND 4
9-21, 9-22	AMEND 1
9-22.1 (REVERSE BLANK)	AMEND 1
9-23 thru 9-25 (REVERSE BLANK)	ORIGINAL
9-27, 9-28	AMEND 1
9-29 thru 9-31 (REVERSE BLANK)	ORIGINAL
10-1, 10-2	ORIGINAL
10-3 thru 10-5 (REVERSE BLANK)	AMEND 1
11-1 thru 11-21	AMEND 4
A-1 thru A-4	AMEND 4
A-5	AMEND 3
A-6	AMEND 4
A-7 thru A-12	AMEND 3
A-13 thru A-16	AMEND 4
A-17 thru A-21	AMEND 3
A-22	AMEND 4
A-23 (REVERSE BLANK)	AMEND 3
B-1	AMEND 4
B-2	ORIGINAL
B-3	AMEND 4
B-4 thru B-10	ORIGINAL

LIST OF EFFECTIVE PAGES

PAGE NUMBERS	EFFECTIVE PAGES
B-11 (REVERSE BLANK)	AMEND 4
C-1 thru C-5 (REVERSE BLANK)	AMEND 4
D-1 thru D-5 (REVERSE BLANK)	AMEND 1
E-1 thru E-4	AMEND 2
F-1 thru F-21 (REVERSE BLANK)	AMEND 3
H-1 thru H-4	AMEND 4
I-1, I-2	AMEND 4
J-1 (REVERSE BLANK)	AMEND 1
K-1 (REVERSE BLANK)	ORIGINAL
L-1, L-2	AMEND 1
M-1 thru M-3	AMEND 4
M-4 thru M-11 (REVERSE BLANK)	ORIGINAL
N-1 thru N-4	AMEND 4
O-1 thru O-3 (REVERSE BLANK)	ORIGINAL
P-1 thru P-3 (REVERSE BLANK)	ORIGINAL
Q-1, Q-2	AMEND 3
R-1, R-2	AMEND 3
S-1 thru S-8	AMEND 4
T-1 thru T-3 (REVERSE BLANK)	AMEND 4
U-1 thru U-4	AMEND 3
V-1 thru V-4	AMEND 4
V-5 thru V-7 (REVERSE BLANK)	AMEND 3
W-1 thru W-7 (REVERSE BLANK)	AMEND 4
W-9 thru W-21 (REVERSE BLANK)	AMEND 4
X-1 thru X-4	ORIGINAL
Z-1 thru Z-3 (REVERSE BLANK)	ORIGINAL
AA-1 thru AA-7 (REVERSE BLANK)	AMEND 4
AB-1 thru AB-3 (REVERSE BLANK)	AMEND 3
AC-1 thru AC-8	AMEND 4
AD-1 thru AD-20	AMEND 4
INDEX-1 thru INDEX-21 (REVERSE BLANK)	AMEND 4

RECORD OF AMENDMENTS

AMEND NUMBER/ IDENTIFICATION	DATE ENTERED (YYMMDD)	ENTERED BY (Signature Rank/Rate, Command Title)
AMEND 1	960521	DCMS, 20 Department Staff
AMEND 2	960521	DCMS, 20 Department Staff
AMEND 3	960521	DCMS, 20 Department Staff
AMEND 4	960521	DCMS, 20 Department Staff

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

ANNEXES:

TABLE OF CONTENTS

TABLE OF CONTENTS

CHAPTER 1 - COMMUNICATIONS SECURITY (COMSEC) MATERIAL CONTROL SYSTEM (CMCS)

CHAPTER 1 - COMMUNICATIONS SECURITY (COMSEC) MATERIAL CONTROL SYSTEM (CMCS)

101. INTRODUCTION TO THE COMSEC MATERIAL CONTROL SYSTEM(CMCS)

a. Communications Security (COMSEC) material is that material used to protect U.S. Government transmissions, communications, and the processing of classified or sensitive unclassified information related to national security from unauthorized persons and that material used to ensure the authenticity of such communications.

b. The protection of vital and sensitive information moving over government communications systems is crucial to the effective conduct of the government and specifically to the planning and execution of military operations. To this end, a system has been established to distribute, control, and safeguard COMSEC material. This system, which consists of production facilities, COMSEC Central Offices of Records (CORs), distribution facilities (i.e., depots), and CMS accounts, is known collectively as the CMCS.

c. COMSEC material is managed in COMSEC accounts throughout the federal government to include departments and civil agencies as well as the civilian sector supporting the federal government.

105. NATIONAL SECURITY AGENCY (NSA). The National Security Agency is the executive agent for developing and implementing national level policy affecting the control of COMSEC material. NSA is also responsible for the production of most COMSEC material used to secure communications as well as the development and production of cryptographic equipment.

110. DEPARTMENT OF THE NAVY (DON). The DON administers its own CMCS which includes Navy, Marine Corps, Coast Guard, and Military Sealift Command (MSC) CMS Accounts. The DON system implements national policy, publishes procedures, establishes its own COMSEC accounts which it refers to as CMS accounts, and provides a COR to account for COMSEC material.

NOTE: THROUGHOUT THIS MANUAL, "DON," FOR COMSEC PURPOSES, APPLIES TO U.S. NAVY, U.S. MARINE CORPS, U.S. COAST GUARD, AND MILITARY SEALIFT COMMANDS UNLESS OTHERWISE INDICATED.

a. **Chief of Naval Operations (CNO)** has overall responsibility and authority for implementation of National COMSEC policy within the DON. The Head, Navy Information Security (INFOSEC) Branch (N652) is the COMSEC resources sponsor and is responsible for consolidating the COMSEC programming, planning and implementation of policy and technical improvements.

b. **Commandant of the Marine Corps (CMS)** is the Marine Corps focal point for requirements and administration of the Marine Corps CMS accounts. The Assistant Chief of Staff, Command, Control, Communications, Computers, and Intelligence (C41), (Code CSB), is the Marine Corps COMSEC resources sponsor and coordinates with CNO, COMNAVCOMTELCOM, and DCMS, in establishing, promulgating and overseeing Marine Corps CMS account management matters unique to the Marine Corps.

c. **Commander, Coast Guard Telecommunications Information Systems Command (COGARD TISCOM)** exercises overall authority for all Coast Guard telecommunications issues, including COMSEC matters. Chief, Secure Telecommunications Branch (OPS4) serves as the principal agent for Coast Guard COMSEC matters. OPS4 promulgates Coast Guard COMSEC policy and exercises service wide management of Coast Guard CMS accounts. OPS4 works in close cooperation with CNO, DCMS, and CMIO Norfolk to ensure that all (R
Coast Guard CMS accounts have the necessary COMSEC resources to operate effectively. OPS4 also coordinates with the other services, DIRNSA, and various civil law enforcement agencies for counternarcotics COMSEC requirements.

d. **Commander, Naval Computer and Telecommunications Command (COMNAVCOMTELCOM)** implements the DON CMS Program.

e. **Director, Communications Security Material System (DCMS)** administers the DON CMS program and acts as the COR for all DON CMS accounts. DCMS performs these specific functions:

(1) Drafts and publishes CMS policy directives, standards, and procedures pertaining to COMSEC material security, distribution, training, handling, and accounting within the DON.

(2) Operates and maintains the DON COR and exercises (R
administrative, operational, and technical control over the COMSEC Material Issuing Office (CMIO) for distribution of COMSEC material.

(3) Develops procedures for and monitors compliance with proper physical storage and account management of COMSEC material.

(4) Monitors compliance with national standards of the Protective Packaging Program for cryptographic keying material.

(5) Reviews requests for and authorizes waivers to physical security requirements and the release of DON COMSEC material to contractors.

(6) Reviews fleet operation plans and coordinates requirements for the acquisition of all COMSEC material and publications for DON commands.

(7) Establishes and disestablishes DON CMS and STU-III COMSEC accounts (SCAs).

(8) Plans distribution of COMSEC material to CMIO (R Norfolk to ensure quantities are sufficient for CMS account requirements, exercises, and contingency operations.

(9) Provides status of Navy COMSEC material to CMS

either assume personal responsibility for routine CMS matters or may designate the responsibility to a senior staff officer (O-4 (or selectee)/GS-12 and above). Officers not meeting the above requirement may not designate a SCMSRO.

130. COMMANDING OFFICER (CO). The CO is responsible for properly administering his/her command's CMS account and ensuring compliance with established policy and procedures. Annex D, written specifically for COs, contains a CMS account assurance checklist for use in assessing command compliance with the provisions of CMS 1.

NOTE: THROUGHOUT THIS MANUAL, RESPONSIBILITIES/DUTIES APPLICABLE TO COMMANDING OFFICERS APPLY EQUALLY TO STAFF CMS RESPONSIBILITY OFFICER'S AND OFFICER-IN-CHARGE (OIC), UNLESS OTHERWISE INDICATED.

135. CMS ACCOUNT. A CMS account is an administrative entity, identified by a six-digit account number, in which custody and control of COMSEC material are maintained.

140. CMS CUSTODIAN. An individual designated in writing by the CO to manage COMSEC material issued to a CMS account. The CMS Custodian is the CO's primary advisor on matters concerning the security and handling of COMSEC material and the associated records and reports.

145. ALTERNATE CUSTODIAN(S). The individual(s) designated in writing by the CO responsible for assisting the CMS Custodian in the performance of his/her duties and assuming the duties of the CMS Custodian in his/her absence. Alternate Custodian(s) share equally with the CMS Custodian the responsibility for the proper management and administration of a CMS account.

150. LOCAL HOLDER (LH) ACCOUNT. LH accounts are separate units or commands that require COMSEC material and function essentially as subaccounts of a numbered CMS account. LH accounts are managed in much the same way as a CMS account except they are not assigned a CMS account number and normally receive their COMSEC material from a parent CMS account instead of directly from CMIO Norfolk or other source. (R

155. LOCAL HOLDER CUSTODIAN AND ALTERNATE(S) are individuals designated in writing by the Commanding Officer to manage the COMSEC material issued to a LH account.

NOTE: THROUGHOUT THIS MANUAL, THE USE OF THE TERM "CUSTODIAN" WILL APPLY TO ACCOUNT CUSTODIANS AND THEIR ALTERNATES AS WELL AS TO LH CUSTODIANS AND THEI R ALTERNATES, UNLESS OTHERWISE INDICATED.

160. CMS CLERK. An individual designated in writing by the CO who assists the CMS Custodian and Alternate(s) with routine administrative account matters. Appointment of a CMS Clerk is not mandatory, but is at the **discretion** of the CO.

165. CMS USER. An individual designated in writing by the CO who, regardless of whether or not they personally signed for COMSEC material, requires COMSEC material to accomplish an assigned duty and has obtained the material from a Custodian or another User on local custody. CMS Users must comply with the procedures for the handling and accountability of COMSEC material placed in their charge.

170. CMS WITNESS. Any properly cleared U.S. Government employee (military or civilian) who may be called upon to assist a Custodian or User in performing routine administrative tasks related to the handling of COMSEC material. A witness must be authorized, in writing, access to keying material.

CHAPTER 2 - INTRODUCTION TO COMSEC MATERIAL

201. GENERAL:

a. COMSEC material must be handled and safeguarded based on its assigned classification and accounted for based on its accountability legend (AL) code.

b. COMSEC material control within the U.S. Government is based on a system of centralized and local accounting and decentralized custody and protection. COMSEC material is centrally accountable to DCMS and/or accounted for locally at the account command.

c. COMSEC material enters the DON CMCS when:

(1) NSA produces and transfers keying material to DON CMS accounts for use or distribution (e.g., by CMIO Norfolk). (R

(2) A possession report is submitted for COMSEC material which is in the possession of a Custodian but which is not charged to his/her account (e.g., found COMSEC material).

(3) Material is received by a DON Custodian from another department, agency, foreign government, international organization, or other non-Navy CMS accounts (e.g., equipment received from a civilian firm).

205. APPLICATION OF PROCEDURES. Proper and conscientious application of the procedures contained in this publication are intended to provide maximum flexibility, yet ensure proper security and accountability to prevent the loss of COMSEC material and the possible compromise of the information it protects.

210. LIMITATIONS. This publication cannot address every conceivable situation that might arise in the daily handling of COMSEC material. When unusual situations confront a Custodian or User of COMSEC material, the basic tenets applicable to the protection of classified information should be implemented until definitive guidance is provided by DCMS or other authoritative source (e.g., material's controlling authority, FLTCINC, ISIC).

215. CONTROL AND REPORTING. Control of COMSEC material is based on the following:

a. A continuous chain of custody receipts using both transfer reports and local custody documents.

b. Accounting records, such as periodic inventory reports, destruction records, transfer reports, and local custody records.

c. Immediate reporting of COMSEC material incidents to ensure compromise decisions are made expeditiously by controlling/evaluating authorities.

220. COMSEC MATERIAL 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.

225. COMSEC MATERIAL IDENTIFICATION

a. SHORT TITLE: An identifying combination of letters and/or digits (e.g., KG -84A, USKAT 2333) assigned to certain COMSEC material to facilitate accounting and control. A short title consists of 5 fields:

(1) System: First field consists of a group of letters and/or digits (e.g., KAM, KG, USKAK, AKAT).

(2) Class: Second field consists of letters and/or digits found between the system and the number of a short title. For example, in the short title "USKAC D 166," the "D" is the class. (NOTE: Absence of a letter and/or digit in this field indicates a short title does not have a class which is true for the majority of short titles).

(3) Number: Third field consists of a group of digits immediately after the system and/or the class. For example, in the short title "AKAC 874," the number is "874."

(4) Edition: Fourth field consists of a group of character(s) immediately after the number. For example, in the short title "USKAT 12479 BD," the edition is "BD."

(5) Amendment: The fifth and final field of a short title reflects amendments to publications, modifications to equipment, or equipment mode designators. For example, in the short title "KY -75 MOD 01," the amendment field reflects the modification as "MOD 01." (NOTE: Keying material will not have an amendment field.)

b. ACCOUNTING (serial/register) NUMBER: Most COMSEC material is assigned an accounting (serial/register) number at the point of origin to facilitate accounting and/or inventory functions.

SHORT TITLE EXAMPLE: USKAC D 166 BC 18

System: USKAC
Class: D
Number: 166
Edition: BC
Amendment: Not used in this example.
Serial: 18

c. Figure 2-1 contains information and a chart that can be used to determine the meaning of the two-letter digraph (that precedes the short title) that appears on segmented keying material packaged in canisters. This information also appears on the back of the CMS 25 in Chapter 7 (Figure 7-1).

230. ACCOUNTABILITY LEGEND (AL) CODES

a. Accountability Legend (AL) codes determine how COMSEC material is accounted for within the CMCS. Three AL codes are used to identify the minimum accounting controls required for COMSEC material. The degree of accountability required for each AL code is explained below: (R

(1) AL Code 1: COMSEC material is continuously accountable by accounting (serial/register) number from production to destruction.

(2) AL Code 2: COMSEC material is continuously accountable by quantity from production to destruction.

D)

(3) AL Code 4: COMSEC material is locally accountable by quantity and handled/safeguarded based on its classification after initial receipt to DCMS.

b. CMIO Norfolk is required to continuously account to DCMS for all AL 4 material. All transfers of AL 4 material to or from a CMIO, cache, or a non-DON account must be reported to DCMS. (R

c. AL codes are assigned by the originating government department or agency that produces the COMSEC material and represent the minimum accounting standard.

d. AL codes will appear on all accounting reports but not necessarily on the material.

e. If DCMS changes the AL code for any COMSEC material, the material must be accounted for based on its new AL code effective upon notification of the change.

f. The classification of COMSEC material has no bearing on (R the AL code assigned to an item. For example, Top Secret COMSEC material may be assigned AL 1; however, there is also Secret, Confidential, and Unclassified COMSEC of material that is assigned AL 1. AL codes determine how material is accounted for and classifi cation determines handling and storage requirements.

g. The DCMS COR computer system, NKDS (Navy Key Distribution System), requires assignment of an AL code to each short title in the system to permit automated processing (i.e., automatic distribution and report generation require ments).

(1) As a result, some COMSEC -related items (e.g., NAG 16, CMS 1, CMS 5A) will have AL 4 assigned to them for processing/distribution purposes only. In other words, the DCMS or CMIO originated SF 153 transfer report will identify these items as AL 4, but they are not accountable as COMSEC material and will not appear on an inventory.

(2) COMSEC -related items are to be handled and safeguarded based on their assigned classification.

NOTE: OPNAVINST 5510.1 (series) defines handling and accounting requirements for classified information and SECNAVINST 5720.42 (series) for FOUO and unclassified information.

235. CRYPTO MARKING

The marking or designator "CRYPTO" identifies all COMSEC keying material which is used to protect or authenticate classified or sensitive unclassified government or government -derived information, the loss of which could adversely affect national security. The marking "CRYPTO" is not a security classification.

240. CONTROLLED CRYPTOGRAPHIC ITEM (CCI)

Controlled Cryptographic Item (CCI) is the designator which identifies secure telecommunications or information handling equipment, or an associated cryptographic component, which is unclassified but controlled within the CMCS.

245. STATUS OF COMSEC MATERIAL

a. The usability of COMSEC material is determined by its status (i.e., one of three possible conditions). Status for COMSEC material is assigned at the direction of the controlling authority or originator of the material.

b. The status for equipment and non -keying material items is changed infrequently as they are used for extended periods of time. This material is in effect until it is replaced or superseded.

c. The status for COMSEC keying material is promulgated repeatedly as its lifespan can vary from hours to an indefinite period of time. Most keying material is superseded on a regular or routine basis due to operational use. COMSEC keying material will, at all times, be in one of three status conditions:

(1) Reserve: Held for future use. (See Note 2 below).

(2) Effective: In use to support an operational requirement.

(3) Superseded: No longer authorized for use; must be immediately destroyed.

NOTE: 1. An edition of COMSEC keying material is one in a series of printings of the same short title. Each edition has its own effective period and contains different key variables divided into parts, known as segments. Each segment within an edition will have a designated effective period (i.e., daily, weekly, monthly, bi -monthly, etc.) assigned to it based on the key's crypto -equipment.

2. Some keying material (e.g., Inter -Theater COMSEC Package (ICP)) may be categorized as being in a contingency status. Material in this category is defined as material held for use under specific operational conditions or in support of specific contingency plans. Status documents (e.g., CMSR) will reflect this material as when directed (WHEN DI).

250. COMSEC MATERIAL SUPERSESSION

Supersession refers to a time when a particular item of COMSEC material is no longer eligible for use. COMSEC material is superseded in one of three ways:

a. **Regular supersession**: Supersession based on a specific, pre -determin ed supersession date for each edition of material. For example, each edition of a monthly keytape is superseded on the first day of the month after its implementation; each edition of ten -day material is superseded on the 11th, 21st, and the 31st of the month.

b. **Irregular supersession**: Supersession that is not pre-determined but which occurs as a result of use. Editions and individual segments of irregularly superseded COMSEC material are to be destroyed after the material has been used operationally, when the controlling authority directs

supersession, or, in the case of maintenance key, it may be used until the key becomes unserviceable. Irregular supersession is normally associated with one -time pads, test key, maintenance key, publications, and equipment.

c. **Emergency supersession**: An unplanned change of supersession, usually as a result of a compromise.

255. SOURCES OF SUPERSESSION INFORMATION

The supersession or status of COMSEC material held by CMS accounts can be determined using the following sources:

a. **CMSR**: (R

(1) The CMSR is classified SECRET (NOFORN) and is updated by DCMS on a monthly basis and contains a composite listing of most COMSEC material distributed to DON CMS accounts.

(2) As the CMSR shows the status for the material listed thereon, the CMSR must be held by every DON CMS account that holds COMSEC keying material .

(3) The CMSR shows the short title, long title, controlling authority, AL code (if applicable), status (i.e., effective and supersession date, or reserve (i.e., when directed (WHENDI)), classification, and disposition code.

(4) The CMSR is not COMSEC material and is to be accounted for/handled based on its classification after receipt.

(5) Annex E contains a portion of a typical page of a CMSR and an explanation for the various elements and abbreviations appearing thereon.

NOTE: The CMSR is available on -line via the COMSEC Automated Reporting System (CARS). Viewing the CMSR via CARS provides the most up -to date status information on COMSEC material. Annex F contains the procedures for accessing CARS.

NOTE: In the event of conflicting information with regard to the status of or authorization to destroy COMSEC material, Custodians must use the most recent information available or contact DCMS//30// for guidance.

b. **AMSG-600**: AMSG -600 contains status information for NATO COMSEC material and must be held by every DON CMS account which holds NATO material. AMSG -600 takes precedence over the CMSR in case of conflicting information for NATO COMSEC material.

c. **Joint Staff ICP Manager MacDill AFB, FL**: Status information for keying material designated for use in the Inter-theater COMSEC Package (ICP) is promulgated by a series of GENSER messages using a pre-determined date-time-group (DTG). Joint Staff ICP Manager MacDill AFB, FL distributes this information as shown below (read DTG, Address Indicator Group (AIG), subject, and frequency):

	DTG	AIG	Subject	Frequency
(1)	varies	8712	USKAT-5360	yearly
(2)	211600Z	7863	Conventional package	monthly
(3)	211602Z	901	SOC package	monthly
(4)	211603Z	7092	KEYMAT usage	monthly
(5)	211604Z	902	TRI-TAC	monthly
(6)	211605Z	906	KG-84	monthly
(7)	211607Z	8721	JTAO package	monthly
(8)	211611Z		CENTCOM AOR ICP Usage	monthly
(9)	211612Z	8709	IFF package	monthly
(10)	211612Z	904	Subsurface Fleet COMSEC Message	monthly
(11)	211613Z	903	Weather KEYMATS	monthly

d. **CJCSI 3260.01**. A limited number of commands are authorized to hold two-person controlled (TPC) Sealed Authentication Systems (SAS) keying material. (R

(1) Policy and procedures for handling this material are contained in CJCSI 3260.01. The DCMS role for TPC or SAS material is limited to accounting functions only. (R

(2) Status information for SAS material is promulgated by JCS message and is not listed on the CMSR. Type Commanders also promulgate status information for SAS material. For example, COMSUBPAC and COMSUBLANT disseminate a monthly message to the collective address group (CAG), "SUBPAC" and "SUBLANT," which lists the latest SAS related messages promulgated by theater Commanders. (R

e. **General Message from Controlling Authority**. Status information is also promulgated by controlling authorities via GENERAL messages (e.g., ALCOM, ALCOMPAC P, ALCOMLANT A). (R

NOTE: CMS Custodians are strongly encouraged to coordinate with the servicing communications facility to establish procedures which will ensure that all messages pertaining to COMSEC material are delivered in a timely manner.

260. CATEGORIES OF COMSEC MATERIAL

COMSEC material consists of aids and hard ware which secure telecommunications or ensure the authenticity of such communications. COMSEC material includes, but is not limited

to, COMSEC key, items which embody or describe COMSEC logic, and other items which perform COMSEC functions. COMSEC material is divided into three categories: keying material, equipment, and related information.

a. **Keying Material**: A type of COMSEC aid which supplies either encoding means for manual and automanual cryptosystems or key for machine cryptosystems. Keying material may or may not be marked or designated "CRYPTO." Keying material includes both paper, which may be extractable or non-extractable, and non -paper items.

(1) Paper keying material includes keylists, keytapes, codes, authenticators (includes Identify Friend or Foe (IFF)), one-time tapes, and one -time pads. Keying material can be designated for use as operational, exercise, test (on -the-air), maintenance (off -the-air), or training (off -the-air (e.g., classroom)). The majority of keying material bears the following types of short titles:

Keylists	(AKAK/USKAK)
KeyTapes	(AKAT/USKAT)
Codes	(AKAC/USKAC)
Authenticators	(AKAA/USKAA)
One-time Pads	(AKAP/USKAP)

(a) Extractable keying material is designed to permit the extraction and removal of individual segments of key for hourly, daily, weekly, etc., use. Individual segments are indicated by perforations, dotted lines, or similar separations to permit removal. Some examples of extractable keying material are keytapes, and authentication systems consisting of hourly or daily authentication tables.

(b) Non-extractable keying material is designed to remain intact throughout its entire effective period. An example of non -extractable keying material is operations or numeral codes with separate encode and decode sections.

NOTE: Extractable/non -extractable as used above refers to the physical condition of paper keying material and not the removal or extraction of key from a device either physically or electronically.

(2) Non-paper keying material includes electronically generated key, keying plugs, keyed microcircuits, floppy disks, magnetic tapes, and keying material in solid state form such as programmable read-only memories (PROMs), read-only memories (ROMs), metallic oxide semi-conductor (MOS) chips, and micro-miniature tamper protection systems (micro-TPS).

b. **COMSEC Equipment**: Equipment designed to provide security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor and subsequently by reconverting such information to its original form for authorized recipients, as well as equipment designed specifically to aid in, or as an essential element of the conversion process.

c. **COMSEC-Related Information**: Includes policy, procedural, and general doctrinal publications (e.g., CMS 1, CMS 5A), equipment maintenance manuals (e.g., KAM-410) and operating instructions (e.g., KAO-207), call signs, frequency systems, and miscellaneous material not listed above (e.g., CMSR, NAG 16, DCMS-Generated SF 153).

NOTE:

1. Selected limited maintenance KAMs are being/have been replaced by limited maintenance manuals (LMMs). LMMs are unclassified and are not accountable as COMSEC or COMSEC-related material.
2. Status information on LMMs will be promulgated by DCMS//30//.
3. LMMs will have a Technical Manual Identification Number (TMIN) and a National Stock Number (NSN) assigned to them. LMMs may be requested from:

Aviation Supply Officer
Naval Publications and Forms Directorates
5801 Tabor Avenue (Code 1013)
Philadelphia, PA 19120-5099

DIGRAPHS ON SEGMENTED KEYING MATERIAL PACKAGED IN CANISTERS

1. General: COMSEC keying material packaged in canisters has a preprinted digraph, consisting of two letters, printed to the left of the short title (e.g., " AA" USKAT 1000 BG 1234) on each extractable segment of the tape leader. The two letters are read left to right and provide the following information:

a. First letter: Identifies the number of different key settings within the canister, the number of copies of each key setting, and the total number of segments in the canister, respectively.

b. Second letter: Identifies the cryptoperiod.

2. Use the following chart to determine the meaning of the digraph appearing on segmented keying material packaged in canisters:

1ST LETTER

	KEYS	COPIES OF KEYS	TOTAL SEGMENTS
A	31	1	31
B.	5	3	15
C.	1	5	5
D.	6	5	30
E.	5	1	5
F.	1	10	10
G.	16	1	16
H.	1	31	31
I.	1	15	15
J.	26	1	26
K.	6	12	72
L.	35	1	35
M.	2	1	2
N.	Contact Controlling Authority		
P.	1	45	45
Q.	34	1	34
R.	4	5	20
S.	75	1	75
T.	12	1	12
U.	65	1	65
V.	62	1	62
W.	1	65	65
Y.	26	2	52
Z.	15	5	75

2ND LETTER

A.	Daily (24 hours)
B.	Weekly (7 days)
C.	Monthly
D.	Special mission; not to exceed 24 hours
E.	No prescribed cryptoperiod
F.	Three months
G.	Yearly
H.	Contact Controlling Authority
I.	Six months
J.	Monthly beginning on 1st day used

FIGURE 2-1

(REVERSE BLANK)

CHAPTER 3 - CMS EDUCATION, TRAINING, AND INSPECTIONS

CHAPTER 3 - CMS EDUCATION, TRAINING, AND INSPECTIONS

301. GENERAL

a. CMS Advice and Assistance (A&A) Training Team personnel should be viewed as a CMS Custodian's right -hand asset. Their training and experience provide a readily available source of technical expertise in all areas related to COMSEC material. Their charter ----to train and assist ----should be used advantageously at every opportunity by every command handling COMSEC material.

b. Education and training are available on a worldwide basis to provide basic skills required to fulfill Custodian responsibilities and to assist/train personnel in the procedures required to properly manage a CMS account. These efforts include:

(1) CMS Custodian Course of Instruction (COI) (A -4C-0014).
(2) CMS Local Holder (LH) Custodian COI (A -4C-0031).
(3) Training and assistance provided by CMS A&A Training Teams.

305. CMS CUSTODIAN COURSE OF INSTRUCTION (COI)

a. General: The CMS Custodian COI provides personnel the basic skills necessary to fill a CMS Custodian or CMS Clerk position. The CMS Custodian COI is a five -day course of instruction, emphasizing CMS accounting and reporting requirements to include ANCRS and CARS.

b. Locations: The CMS COI is offered in the following areas:

(1) CONUS East Coast:

(a) Naval Education & Training Center, Newport, RI
(b) Naval Submarine School, Groton, CT
(c) Fleet Training Center, Norfolk, VA

D)

(d) Trident Training Facility, Kings Bay, GA
(e) Fleet Training Center, Mayport, FL

(2) CONUS West Coast:

(a) Trident Training Facility, Bangor, WA
(b) Fleet Training Center, San Diego, CA
(c) Submarine Training Facility, San Diego, CA

(3) EUROPE. Naval Computer Telecommunications Area Master Station MED Det, Rota, Spain

(4) PACIFIC:

(a) Afloat Training Group, Middle Pacific (MIDPAC), Pearl Harbor, HI

(b) Afloat Training Group, Yokosuka, Japan

c. Quotas: Quotas for the CMS Custodian COI are available from each of the sites and should be coordinated through the command CMS Custodian and Training Officer.

d. Criteria for Attending: Criteria for attending the CMS Custodian COI are:

(1) U.S. citizenship (includes naturalized)
(2) SECRET security clearance
(3) E-6/GS-7 and above (Custodians only)
(4) Six months of government service
(5) Be assigned to or designated to fill a CMS Custodian or CMS Clerk position

NOTE: LH Custodians/Alternates are not authorized to attend the CMS Custodian COI.

e. Recommendations for improvements in the course curriculum may be forwarded to:

CMS Custodian COI (A-4C-0014)
Model Manager (ATTN: NETC 36)
Naval Education and Training Center
Newport, RI 02841-1206

310. CMS LOCAL HOLDER (LH) CUSTODIAN COURSE OF INSTRUCTION (COI)

a. General. The CMS LH Custodian COI provides personnel the basic skills necessary to fill a CMS LH Custodian position. The CMS LH Custodian COI is a three-day course of instruction, emphasizing management of a CMS LH account and operation of the data transfer device (DTD).

b. Locations/Quotas: Same as Article 305.b. and c., respectively.

c. Criteria for attending: Same as Article 305 d. except that attendance is for personnel assigned to or designated to fill a LH CMS Custodian position.

d. Recommendations for improvements in the course curriculum may be forwarded to: CMS LH Custodian COI (A-4C-0031) using the address in Article 305 e.

315. CMS TRAINING VISITS AND CMS INSPECTIONS

a. CMS Training Visits : All CMS accounts and their associated LHs are required to receive a CMS A&A Training Visit every 18 months . The 18 month requirement may be waived by an ISIC if a ship or submarine is in an overhaul period. **(NOTE:** Article 325 contains additional information on CMS Training Visits.)

b. CMS Inspections : All CMS accounts must undergo a formal CMS Inspection every 24 months . This inspection will be unannounced and conducted in accordance with the procedures contained in CMS 3 (series).

320. CMS A&A TRAINING TEAMS

a. CMS A&A Training Teams constitute a worldwide network of CMS subject matter experts. They were established to provide assistance and training to personnel assigned CMS responsibilities. Training may be conducted at the account command or at the facility of the area CMS A&A Training Team.

b. Specific training topics are scheduled by the Training Team offices at established intervals and cover both general and specific subjects of interest to COs, OICs, SCMSROs, ISICs, CMS Inspectors, CMS Custodians and Users.

c. CMS A&A Training Team assistance is limited to CMS (R issues only, and not the operational aspects of communications or cryptology. (**NOTE**: CMS 2 details Advice and Assistance (A&A) Program and is only provided to servicing A&A Teams. Specific assistance may be requested by contacting your A&A Team.)

325. CMS A&A TRAINING TEAM SERVICES

a. General : CMS A&A Training Teams can provide assistance in resolving general or specific problems and in most cases this can be done over the telephone. When required, a date can be arranged for a Training Team to visit a command.

b. Request for Service (s): Submit a request for service(s) to the closest CMS A&A Training Team in your area (See Article 330 for CMS A&A Training Team locations).

c. Types of Services : CMS A&A Training Teams provide the following services:

(1) CMS TRAINING VISITS :

(a) Training Visits provide the basis for self-improvement and are not to be confused with a formal CMS

Inspection. Training Visits last six to eight hours, are strictly informal, and provide guidance on the policy and procedures for COMSEC material.

(b) Results of a Training Team visit are not reported outside of the command visited. A debrief to the Commanding Officer (or designated representative) and the Custodian is provided covering specific areas of training and the personnel involved.

(c) Training Visits encompass the CMS account, its LHs, and Users. (NOTE: Training for LH accounts and their Users must be coordinated and scheduled by the parent CMS account with the CMS A&A Training Team.)

(2) CMS FOR COMMANDING OFFICERs :

This training is for COs, SCMSROs, and OICs to enable them to effectively monitor their account's compliance with established procedures. Training lasts approximately two hours and may be conducted at the account command or other location as coordinated by the requesting command.

(3) CMS INSPECTOR CERTIFICATION/RECERTIFICATION :

(a) CMS Inspectors must be retrained every 36 months to maintain their authorization to inspect CMS accounts.

(b) This training enables ISIC staff representatives to conduct formal CMS Inspections of subordinate account commands.

(c) CMS Inspector training is conducted by all A&A Training Teams except for NCTAMS MED Det Rota.

(d) CMS Inspector training consists of 8 hours of classroom training instruction and participation in a minimum of one A&A Training Visit or assist in an actual CMS Inspection.

(e) DCMS issues CMS Inspector Certificates based on the recommendation of the A&A Training Teams.

(4) CMS USER WORKSHOPS :

Provides CMS Custodians with supplemental training for their Users. This training lasts approximately three hours and can be provided at the account command or at the CMS A&A Training Team site.

(5) CMS SEMINARS :

Addresses changes to CMS policy and procedures, recurring problems in account management, insecurity trends and topics of concern introduced by attendees. CMS Seminars are primarily for COs, CMS Inspectors, and CMS Custodians. Seminars are conducted semi-annually and hosted by either an ISIC or an area CMS A&A Training Team.

(6) STU-III BRIEFS :

Provides guidance and training on STU -III policy and procedures for the handling and safeguarding of STU -III Type I material held by DON CMS accounts only.

(7) AUTOMATED CMS SYSTEMS :

CMS A&A Training Team personnel can provide training and assistance on the following automated systems:

(a) Automated Navy COMSEC Reporting System (ANCRS)

ANCRS is a software program which permits CMS Custodians to maintain their account records and generate CMS reports using a personal computer (PC).

(b) COMSEC Automated Reporting System (CARS)

CARS provide s a method for electronically transferring CMS reports and CMS -related information in the form of ASCII files to and from the DCMS database using a PC and a STU -III. CARS requires an IBM -compatible PC, a STU -III, word processing software, and VSTERM communications software. Annex F contains procedures for accessing/using CARS.

(8) VIDEO CASSETTE LIBRARY . Each CMS A&A Training Team maintains a library of VHS tapes covering a variety of CMS topics to supplement area training efforts or for use as training material at remote locations that are not visited on a regular basis. Contact your area CMS A&A Training Team office for a list of available tapes.

330. AREAS OF RESPONSIBILITY FOR CMS A&A TRAINING TEAMS . CMS A&A Training Team responsibilities are divided among 10 teams, each responsible for a specific geographical region as shown below:

a. **ATLANTIC REGION** (R

(1) DCMS Washington, DC . Delaware, Maryland, Pennsylvania, Northern Virginia (including Quantico & Dahlgren), West Virginia, and the District of Columbia.

(2) NCTAMS LANT Norfolk, VA . Guantanamo Bay, Iceland, Illinois, Indiana, Iowa, Kentucky, Michigan, Minnesota, Missouri, North Carolina, Ohio, Oklahoma, Tennessee, Dallas/Fort Worth, Texas, Virginia (less Northern Virginia, Dahlgren, and Quantico), and Wisconsin.

(3) NTCC Mayport, FL . Alabama, Arkansas, Caribbean (Andros Island Test Range), Cuba, Florida, Georgia, Lesser Antilles, Louisiana, Mississippi, Panama, Puerto Rico, South Carolina, and Texas (less Dallas/Fort Worth),

(4) NCTS Newport, RI . Connecticut, Maine, Massachusetts, New Hampshire, New Jersey, New York, Rhode Island, Vermont, and Newfoundland.

b. **PACIFIC REGION**

(1) NCTAMS EASTPAC HONOLULU, HI . ALL EASTPAC, Hawaii, and Australia.

(2) NCTS SAN DIEGO, CA . Arizona, California, Colorado, Kansas, New Mexico, Nevada, and Utah.

(3) NCTC PUGET SOUND, WA . Alaska, Idaho, Montana, Nebraska, North Dakota, Oregon, South Dakota, Washington, and Wyoming.

(4) NCTS YOKOSUKA, JAPAN . Japan, Korea, Marianas Islands, Philippines, and all WESTPAC between 060E and 165E (less Australia).

c. **EUROPEAN REGION**

(1) NCTAMS MED DET, ROTA, SPAIN . Azores, Spain, and European theater (shared with NCTAMS MED).

(2) NCTAMS MED NAPLES, ITALY . Indian Ocean (West of 060E), Italy, Persian Gulf, and European theater (shared with NCTAMS MED DET Rota).

CHAPTER 4 - ESTABLISHING A CMS ACCOUNT AND CMS RESPONSIBILITIES

CHAPTER 4 - ESTABLISHING A CMS ACCOUNT AND CMS RESPONSIBILITIES

CHAPTER 4 - ESTABLISHING A CMS ACCOUNT AND CMS RESPONSIBILITIES

401. REQUIREMENT FOR A CMS ACCOUNT

An organization that requires COMSEC material must obtain such material through a CMS account managed by a designated CMS Custodian. When it is not possible to draw needed COMSEC material from an existing CMS account (either within the organization or located in close proximity thereto), the requirement to establish a new CMS account must be validated by the organization's Immediate Superior in Command (ISIC).

405. ESTABLISHING A CMS ACCOUNT

a. Preparation:

(1) Prior to establishing a CMS account, an organization must coordinate with its ISIC and determine its required COMSEC material holdings.

(2) Additionally, a physical security inspection of the area(s) being designated for storage of COMSEC material must be conducted to ensure compliance with the minimum physical security requirements for safeguarding COMSEC material. Physical security requirements are contained in Chapter 5 and Annexes M, N, O, and P.

b. Validation of Authorized Holdings:

The distribution of all COMSEC material requires authorization from the controlling authority (CA) of the material. Validation requirements are as follows:

(1) Navy shore units must obtain CA validation for COMSEC material required by their account.

(2) Navy, surface and sub -surface, and Coast Guard surface units do not require CA validation for COMSEC material contained in the standard fleet allowance instructions (i.e., CINCLANTFLT/CINCPACFLT/CINCUSNAVEURINST C2282.1 (series), COMSUBLANTNOTE C2280 (series)), and Coast Guard area instructions (i.e., PAC/LANTAREAINST C2282.1 (series)).

NOTE: ISICs are responsible for obtaining CA validation for COMSEC material that is not listed in fleet instructions as part of the standard allowance for a command.

(3) USMC Fleet Marine Forces and all Coast Guard commands must have their COMSEC material holdings validated by the Commander, Marine Force (COMMARFOR) LANT or PAC, and Commander, COGARD TISCOM, respectively.

(4) USMC supporting establishments (i.e., bases, posts, and stations) must have their COMSEC material holdings validated by their ISIC.

c. Lead Time to Establish: At least 45 days is required to establish a CMS account and to provide the initial COMSEC material. Initial issue will be determined by DCMS based on availability of the required COMSEC material.

d. Request to Establish:

(1) A letter or message must be submitted to establish a CMS account. Letters must be signed by the Commanding Officer or "Acting" Commanding Officer. (**NOTE**: Correspondence signed "By direction" is not acceptable.)

(2) Annex H contains a sample request listing all the required data for establishing a CMS account.

(3) Address a CMS account establishment reques t as follows:

(a) Navy and MSC Commands:

Submit to DCMS//30//, info ISIC, administrative Chain of Command, NAVELEXCEN PORTSMOUTH//270//, CMIO, and CAs of all required COMSEC material.

(b) Marine Corps Commands:

Submit to Commandant Marine Corps//CSB//, info DCMS//30//, administrative Chain of Command, NAVELEXCEN PORTSMOUTH //270//, CMIO, and CAs of all required COMSEC material.

(c) Coast Guard Commands:

Submit to Commander, COGARD TISCOM//OPS4//, info COMLANTAREA COGARD or COMPACAREA COGARD, DCMS//30//, administrative Chain of Command, NAVELEXCEN PORTSMOUTH//270//, CMIO, and CAs of all required COMSEC material.

(d) Naval Reserve Commands:

Submit to COMNAVRESFOR//01A2//, info DCMS//30//, administrative Chain of Command, NAVELEXCEN PORTSMOUTH//270//, CMIO, and CAs of all required COMSEC material.

e. Identification of Required Material:

All COMSEC material (i.e., keying material, equipment and related devices, cryptographic system operating instructions (KAOs) and maintenance manuals (KAMs), etc.) must be specifically identified by short title and desired quantity.

f. DCMS Action:

DCMS will establish a CMS account based on the information contained in the request, assign a six -digit CMS account number, and direct distribution of the required material.

g. Steps Required to Establish a CMS account:

(1) ISIC validate requirement for a CMS account to approving authority identified in Article 405 d.

(2) ISIC validate command compliance with physical security safeguards for the storage of COMSEC material to approving authority identified in Article 405 d.

(3) ISIC determine the required COMSEC material.

(4) Command/ISIC, obtain CA authorization in accordance with Article 405 b.

(5) CO designate, in writing, a qualified CMS Custodian and Alternate Custodian(s).

(6) Command submit request for account establishment and required COMSEC material.

h. Actions required to ensure recipt of COMSEC material (after an establishment request has been approved):

(1) The account Custodian must coordinate with the area Defense Courier Service (DCS) station and establish a DCS account by submitting a DCS Form 10. DCS Manual 5200.1 (series) contains the administrative and operational procedures of the DCS.

NOTE: Commands must ensure that DCMS//30// is informed of their DCS address upon initial establishment of courier service and whenever there is a change in their DCS address.

(2) The account Custodian must submit a CMS Form 1 listing Custodian personnel only to CMIO in order to receipt for and courier COMSEC material for their command. Annex I contains instructions for CMS Form 1 and a sample CMS Form 1.

410. SELECTION OF CMS CUSTODIAN PERSONNEL

A CMS account or LH account must have a designated Cus todian and a minimum of one Alternate. Individuals selected should:

a. Be responsible individuals and qualified to assume the designated custodian duties.

b. Be in a position or level of authority to permit them to exercise proper jurisdiction in fulfilling their responsibilities.

c. Not have previously been relieved of Custodian duties for reason of poor performance.

d. Not be assigned collateral duties which will interfere with their custodian duties. When appointing Custodian personnel, the Commanding Officer must consider the volume, type, and location(s) of COMSEC material in the account, tempo of command and account operations, and Two -Person Integrity (TPI) requirements.

415. DESIGNATION REQUIREMENTS FOR CMS CUSTODIAN PERSONNEL

a. Designation Requirements:

CMS Custodian personnel must be designated in writing by the Commanding Officer and meet the following requirements:

(1) U. S. Citizen (includes naturalized; immigrant aliens are not eligible).

(2) Commissioned Officer, enlisted E -6 or above (or selectee), or civilian government employee GS -7 or above, all of whom must have a minimum of six months government service.

NOTE: Commissioned officers must have at least six months commissioned service (exclusive of duty under instruction or in training), or have six years of enlisted service.

(3) Possess a security clearance equal to or higher than the highest classification of COMSEC material to be held by the account. Appointment can be based on an interim security clearance.

(4) Be authorized access, in writing, to keying material.

(5) The position description of a civilian government employee must specify custodian duties as either full -time or collateral.

(6) Military personnel (except USMC/USCG) must complete CMS Personnel Qualification Standards (PQS) (NAVEDTRA 43462 (series)) SN 0501-LP-478-5600 no later than 45 days after appointment as a Custodian following completion of the CMS Custodian COI.

(7) Meet one of the following for the CMS Custodian COI:

(a) Graduate within 90 days after appointment,

(b) Graduated within the previous 12 months, **OR**

(c) Scheduled to attend the CMS Custodian COI as soon as practicable, and have satisfactorily completed the CMS Custodian Correspondence Course (NAVEDTRA 13075 (series)) within the previous 12 months.

NOTE: 1. Fully qualified p ersonnel who have performed custodian duties within the past 12 months may be re -appointed custodian duties provided that none of the custodian designation requirements were previously waived.
2. A graduate of the CMS Custodian COI (within the last 12 months) may be appointed as a CMS LH Custodian without completing the CMS LH COI.
3. A graduate from the CMS LH Custodian COI may **not** be appointed as a CMS Custodian without completing the CMS Custodian COI.

b. General Designation Policy:

(1) Time limit. There is no restriction on the time an individual may perform custodian duties.

(2) Waivers:

(a) Commanding Officers are authorized to waive the length of government service required for Custodian personnel. Waivers of this requirement must be documented locally and retained by the account and its ISIC until no longer in effect. (**NOTE**: Do not submit copies of these waivers to DCMS.)

(b) Waivers of all other requirements must be submitted as follows:

Type Command:	**Action Addressee**:
Navy (subordinate to FLTCINC)	FLTCINC//N6//
Marine Corps	CMC//CSB//
MSC	COMSC//N62M//
Coast Guard	COGARD TISCOM//OPS4//
Naval Reserve	COMNAVRESFOR//01D//
Navy (not subordinate to a FLTCINC)	DCMS//20//

(3) Alternate Custodian(s). Appointment of more than one Alternate Custodian to a CMS account is recommended. The number of Alternate Custodians (beyond the minimum of one) is left to the **discretion** of the Commanding Officer.

(4) Temporary Assumption of Custodian Duties:

(a) During the temporary absence of the CMS Custodian, the Alternate Custodian must administer the account.

However, the Alternate Custodian may not administer the account for more than 60 days. If the CMS Custodian is absent for more than 60 days, a new CMS Custodian must be appointed.

(b) The Commanding Officer of the account command may authorize an account inventory before, during, or after the temporary absence of the CMS Custodian.

420. DESIGNATION REQUIREMENTS FOR CMS CLERKS, USERS, AND WITNESSES. CMS Clerks, Users, and Witnesses must meet the following requirements:

a. U.S. Government employee who is a natural born or naturalized U.S. citizen.

NOTE: Immigrant aliens, when properly cleared, are restricted to COMSEC material classified CONFIDENTIAL and below. An immigrant alien, regardless of clearance, may not be appointed as a CMS Clerk.

b. Possess a security clearance equal to or higher than the highest classification of the COMSEC material being handled. Appointment can be based on an interim security clearance.

c. Be responsible individuals and qualified to execute his/her assigned CMS duties.

d. Be authorized access, in writing, to keying material.

e. Be designated in writing by the Commanding Officer. (**NOTE**: This requirement does not apply to CMS Witnesses.)

f. Complete applicable CMS PQS Checkoff. (**NOTE**: This requirement does not apply to CMS Witnesses or USMC/USCG personnel.)

425. LETTER/MEMORANDUM OF APPOINTMENT (LOA/MOA)

a. CMS Custodian and Alternate(s), Local Holder Custodian and Alternate(s), and CMS Clerks must be formally designated in an individual Letter or Memorandum of Appointment (LOA/MOA).

b. The LOA/MOA will be signed by the Commanding Officer and maintained locally at the command for a minimum of two years following the relief of an individual. (**NOTE**: Do not forward LOAs/MOAs to DCMS.)

c. LH units must forward a copy of the LOA/MOA to the account CMS Custodian.

d. LOA/MOA must contain name, SSN, grade/rank, date of appointment, CMS school location/completion date, position held,

and security clearance of appointed personnel. Also, each LOA/MOA must identify command title, CMS account number, and a list of waivers that the account and/or Custodian personnel or CMS Clerk have been granted.

e. Annex J contains a sample LOA/MOA for Custodian personnel and CMS Clerks.

430. HIGHEST CLASSIFICATION INDICATOR (HCI)

a. The Highest Classification Indicator (HCI) is used to determine the highest classification of COMSEC material that an account may hold. The HCI is determined by comparing the clearance level of the Custodian personnel and then selecting the highest clearance level they have in common. For example, the CMS Custodian has a Top Secret clearance and the Alternate has a Secret clearance; the HCI for the account is therefore Secret.

b. DCMS maintains the HCI for DON CMS accounts and provides this information to the National Security Agency (NSA).

c. The HCI is checked by the NSA prior to shipping COMSEC material to an account. COMSEC material is released for shipment only after it has been determined that the HCI equals or exceeds the classification of COMSEC material to be shipped.

d. HCI information must be included in a request to establish a CMS account. Thereafter, commands must submit a letter or message to DCMS//30// whenever there is a change in their HCI.

435. CLAIMANCY SHIFT. When a command undergoes a shift in claimancy or a name change, submit a message action to DCMS WASHINGTON DC //30//, information to CMIO Norfolk and Chain of Command, which details the change(s). This information will then be used to update the DCMS COR database. For name and/or address changes, you will also need to update your DCS two-line address by submitting new DCS Form 10(s) to your servicing DCS station. (R

440. CMS RESPONSIBILITIES

a. **Immediate Superior in Command (ISIC)**. ISICs are responsible for the CMS accounts of their subordinate commands by:

(1) Validating the operational requirement for a CMS account.

(2) Determining COMSEC material allowance requirements and, when required, obtaining CA authorization in accordance with Article 405.b.

(3) Ensuring that physical security inspections are conducted.

(4) Conducting CMS account inspections.

(5) Reviewing and/or retaining CMS records pending receipt of DCMS notice of reconciliation upon account disestablishment.

b. Staff CMS Responsibility Officer (SCMSRO):

(1) SCMSROs must be designated, in writing, by the flag officer and have a security clearance equal to or higher than the highest classification of COMSEC material held by the account.

(2) A designated SCMSRO (O -4 (or selectee)/GS -12 and above) is responsible for the proper administration of routine matters for a CMS account.

(3) SCMSROs must sign CMS correspondence and reports as "Staff CMS Responsibility Officer" vice "By direction."

(4) Duties of the SCMSRO cannot be further delegated and must revert to the appointing official in the absence of the assigned SCMSRO.

(5) Specific duties are identical to Commanding Officer duties and responsibilities listed in Article 450. (**NOTES**: Assignment of a SCMSRO does not relieve the appointing official of ultimate responsibility for the proper management of a CMS account. The SCMSRO may delegate two of the CO spot checks (A to the Communications Officer (COMMO), as long as the COMMO is not designated as the CMS Custodian or Alternate.)

c. Chain of Command:

(1) The management and security of COMSEC material are inherent responsibilities of all levels of command. Proper evaluation of CMS administrative procedures can be made only if all officers in the Chain of Command are knowledgeable of and support compliance with established CMS procedures and requirements.

(2) In performing routine duties, the Custodian will normally report to the Communications Officer for functional direction and administration. However, the Custodian must have direct access to the Commanding Officer.

d. CMS Custodian:

(1) The individual designated in writing by his/her Commanding Officer who is responsible for all actions associated with the receipt, handling, issue, safeguarding, accounting, and disposition of COMSEC material assigned to a CMS account.

(2) He/she is responsible to the Commanding Officer for the performance of his/her CMS duties and will normally report to the Communications Officer for functional direction and administration.

e. Alternate CMS Custodian(s):

(1) The individual(s) designated in writing by his/her Commanding Officer who is/are responsible for assisting the CMS Custodian in the performance of CMS duties and for assuming the duties of the CMS Custodian in his/her absence.

(2) Alternate CMS Custodian(s) report to the CMS Custodian for CMS duties and share equally with the CMS Custodian the responsibility for the proper management and administration of a CMS account.

f. Local Holder (LH) Custodian(s):

(1) LH Custodian(s) (and their alternates) are designated in writing by his/her Commanding Officer and are responsible for the proper handling and accounting of the COMSEC material received from the parent CMS account.

(2) LH Custodians, irrespective of command relationships, must adhere to the written instructions issued by the CMS Custodian.

g. CMS User:

(1) CMS users are designated in writing by his/her Commanding Officer and are responsible for the proper security, control, accountability, and disposition of the COMSEC material placed in their charge and must comply with the procedures in this publication and local instructions provided by the issuing source.

(2) All CMS Users must execute a CMS Responsibility Acknowledgement Form as shown in Annex K.

h. CMS Clerk:

(1) CMS Clerks are designated in writing by his/her Commanding Officer and are responsible for assisting Custodian personnel in the execution of administrative duties associated with the management of a CMS account.

(2) Assignment of a CMS Clerk is at the **discretion** of the Commanding Officer.

i. CMS Witness:

(1) A CMS Witness is responsible for assisting Custodian and User personnel in the proper execution of routine administrative tasks related to the handling and safeguarding of COMSEC material (e.g., receipt, destruction, inventory, or maintaining TPI).

(2) A CMS Witness must be familiar with applicable procedures of this manual and all command -issued directives governing the handling of COMSEC material with respect to the task being performed. (NOTE: A CMS User and CMS Clerk may function as a CMS Witness but a witness may not necessarily be a CMS User or Clerk.)

(3) A CMS Witness must be authorized access, in writing, to keying material.

445. LETTER OF AGREEMENT (LOA)

a. In those instances where a LH Custodian or User is responsible to a Commanding Officer other than that of the numbered CMS account command or issuing activity, a Letter of Agreement (LOA) must be executed between the CMS account command and the LH or User command.

b. Annex L contains a sample LOA with the minimum requirements to be addressed.

c. LOAs must be updated with every change of command or every three years, whichever occurs first.

450. CMS RESPONSIBILITIES AND DUTIES: COMMANDING OFFICER

Commanding Officers/OICs are **ultimately** responsible for the proper management and security of all COMSEC material held by his/her command and must:

a. Ensure compliance with established policy and procedures governing the safeguarding and handling of COMSEC material.

b. Appoint, in writing, qualified and responsible individuals as CMS Custodian and Alternate Custodian(s) and, if desired, a CMS Clerk.

c. Establish, in writing, a list of personnel authorized access to keying material.

d. Ensure that training procedures are adequate to meet operational requirements.

e. Ensure that the CMS Personnel Qualification Standards (PQS) (NAVEDTRA 43462 (series)) are incorporated into the command training program for CMS Custodians, Clerks and Users. (NOTE: CMS PQS does not apply to USCG/USMC personnel.)

f. Ensure that CMS incident reports are promptly submitted and action taken as required.

g. Ensure that local procedures are established for identification and reporting of any potentially significant changes in lifestyle, financial status, or disciplinary problems involving personnel authorized access to COMSEC material; and that those changes are reported to the command Security Manager and if appropriate, the Special Security Officer (SSO).

h. Ensure that unannounced spot checks are conducted, at least quarterly, of the CMS Vault and spaces where COMSEC material is used and stored. The CO may delegate **no more than two** of the four quarterly inspections to the XO. (**NOTE:** Annex D contains a checklist which may be used by COs/OICs to assess command compliance with the provision of this manual. The SCMSRO (A may delegate two of the CO spot checks to the COMMO).

i. Receive debriefings from CMS Advice and Assistance (A&A) Training Teams and CMS Inspectors.

j. Ensure that comments on personnel performance of Custodians are included in fitness reports, enlisted evaluations, and civilian performance appraisals, as applicable.

k. Ensure that custodian assignments are documented in an individual's service record or position description, as applicable.

l. Ensure that Emergency Action Plan (EAP) is established and tested. (**NOTE**: Overseas commands are to emphasize emergency destruction plans.) Annex M contains guidance for developing an EAP.

m. Ensure that an inventory of all COMSEC material held by an account is conducted in conjunction with a change of Commanding Officer as required by Navy Regulations (Article 0807), upon change of Custodian, and semiannually as required by this manual.

n. Ensure that assignment of collateral duties to custodian personnel will not interfere with custodian responsibilities.

NOTE: 1. CO responsibilities onboard MSC ships will be performed by the Ship's Master except for T-AGOS (SURTASS) ships where they will be performed by the embarked mission supervisor.

2. A CO whose command includes remote detachments may choose to allow a remote detachment to establish its own independent CMS account. If the title of the separate CMS account states "Detachment" or the equivalent, the responsible authority in charge of the unit is automatically authorized to sign routine CMS documents which would otherwise require the signature of the CO (e.g., CMS accounting inventory or destruction records). The degree of delegation of other command CMS responsibilities is at the discretion of the CO, who may wish to have such a CMS intra-command relationship formally recorded. Such a formal record or description of duties delegated is optional and should not be forwarded to DCMS.

455. CMS RESPONSIBILITIES AND DUTIES: CMS CUSTODIAN

CMS Custodians are responsible to the Commanding Officer through the Chain of Command for the proper management and security of all COMSEC material held at the command and also serve as the Commanding Officer's primary advisor on CMS account management matters. In this capacity, the CMS Custodian must:

a. Provide the Commanding Officer and other interested personnel with information about new or revised CMS policies and procedures and their impact on the command.

b. Acquire, monitor, and maintain the command COMSEC material allowance. This includes an annual review of all COMSEC material holdings to ensure that there is a continuing need for the quantity and types of all COMSEC material held. Material held in excess of operational requirements should be identified by submitting a routine modification to an allowance in accordance with Chapter 6.

c. Maintain proper storage and adequate physical security for the COMSEC material held by the account.

d. Keep Alternate Custodian(s) informed of the status of the account so that the Alternate(s) are, at all times, fully capable of assuming the duties of the CMS Custodian.

e. Provide to LH Custodian(s) and User personnel written guidance or appropriate extracts from this publication concerning the handling, accountability, and the disposition of COMSEC material. Emphasis must be placed on material accountability, TPI requirements, security, and the identification of improper practices.

f. Conduct training to ensure that all personnel handling COMSEC material are familiar with and adhere to proper CMS procedures. The CMS PQS (NAVEDTRA 43462 (series)) is an excellent training tool and is required for use in indoctrinating personnel (less USCG/USMC personnel) in CMS procedures. Document training locally in accordance with command directives.

g. Maintain records and files as required by this manual.

h. Ensure prompt and accurate preparation, signature, and submission of account correspondence, message, and accounting reports.

i. Issue COMSEC material on local custody form(s) after verifying that the recipient is authorized to hold COMSEC material and has executed a CMS Responsibility Acknowledgment Form.

j. Oversee the implementation of and compliance with OTAR/OTAT procedures (e.g., periodic review of local logs, adherence to TPI requirements).

k. Ensure that LHs/Users properly inventory and destroy COMSEC material issued to them through periodic spot checks.

l. Ensure that procedures are established to reassign local custody responsibility for COMSEC material held by individuals permanently leaving the command, and those who are departing on TAD/TDY in excess of 30 days.

m. Ensure that all amendments to this manual and other CMS-related publications are entered promptly and correctly.

n. Maintain the account's portion of the command Emergency Action Plan (EAP). (**NOTE**: Overseas commands must emphasize emergency destruction plans.) Annex M contains guidance for developing an EAP.

o. Conduct required inventories and destruction of COMSEC material in accordance with this manual.

p. Ensure that proper physical security measures are maintained when COMSEC material is transported within the command.

q. Ensure that COMSEC material shipped outside of the command is properly packaged and shipped via an authorized method as required by this manual.

r. Ensure that pagechecks of COMSEC material are conducted as required.

s. Ensure that TPI requirements are maintained in accordance with this manual.

t. Ensure that modifications to COMSEC equipment are promptly and properly performed by qualified individuals in accordance with the guidance in OPNAVINST 2221.3 (series) and that modification residue is disposed of properly.

u. Report immediately to the Commanding Officer any known or suspected insecure practice or CMS incident in accordance with this manual. Initiate action to ensure that required reports are submitted and replacement material is, when required, obtained.

460. CMS RESPONSIBILITIES AND DUTIES: ALTERNATE CUSTODIAN

a. Alternate Custodian (s) are jointly responsible with the CMS Custodian to his/her Commanding Officer for the proper management and security of all COMSEC material held by the command and as such, have the same duties and responsibilities as a CMS Custodian in Article 455.

b. On a continuing basis, the Alternate Custodian(s) must be actively involved in the daily operation of the account and be ready at all times to fully administer the account in the absence of the CMS Custodian.

465. CMS RESPONSIBILITIES AND DUTIES: LOCAL HOLDER CUSTODIAN

Local Holder (LH) Custodian is responsible to his/her Commanding Officer for the proper management and security of all COMSEC material held by the command. LH commands or elements are responsible to the parent account command for the proper accountability, security, control, and disposition of COMSEC material issued to them by the parent CMS account. LH Custodian must also:

a. Provide the Commanding Officer of the LH command or element with information about new or revised CMS policies and procedures and their impact on the command.

b. Follow written instructions issued by the parent account CMS Custodian governing the handling, accountability, and disposition of COMSEC material.

c. Provide written guidance concerning handling, accountability, and disposition of COMSEC material to User personnel. Conduct training to ensure that all personnel handling COMSEC material are familiar with and adhere to proper CMS procedures. Emphasis should be placed on accountability, security, TPI requirements, and the identification of improper practices. Document training locally in accordance with command directives.

d. Ensure proper inventory and destruction of COMSEC material issued to User personnel.

e. Keep the Alternate LH Custodian(s) informed of the status of the account so that the alternate(s) is/are, at all times, fully capable of assuming the duties of the LH Custodian.

f. Ensure that proper storage and adequate physical security is maintained for COMSEC material.

g. Ensure that all amendments to this manual and CMS-related publications are entered promptly and correctly.

h. Complete, maintain, and forward required accounting records and reports to the parent account Custodian.

i. Issue COMSEC material to User personnel on local custody forms after verifying that the recipient is authorized to hold COMSEC material and has executed a CMS Responsibility Acknowledgment Form.

j. Oversee the implementation of and compliance with the OTAR/OTAT procedures (e.g., periodic review of local logs, adherence to TPI requirements).

k. Ensure that pagechecks of COMSEC material are conducted as required.

l. Ensure adherence to TPI requirements.

m. Incorporate emergency destruction procedures for COMSEC material into the LH command Emergency Action Plan (EAP). Refer to Annex M for guidance on an EAP.

n. Report immediately to the LH account Commanding Officer and the parent account CMS Custodian any known or suspected insecure practice or COMSEC incident in accordance with this manual. Coordinate with the parent account CMS Custodian to ensure that required reports are submitted and replacement material is, when required, obtained.

470. CMS RESPONSIBILITIES AND DUTIES: ALTERNATE LH CUSTODIAN

a. Alternate LH Custodian(s) are jointly responsible with the LH Custodian to his/her Commanding Officer as well as to the parent account CMS Custodian for the proper management and security of all COMSEC material held by the command and as such, have the same duties and responsibilities as the LH Custodian in Article 465.

b. On a continuing basis, the Alternate LH Custodian(s) must be actively involved in the daily operation of the account and be ready, at all times, to fully administer the account in the absence of the LH Custodian.

475. CMS RESPONSIBILITIES AND DUTIES: CLERK

a. CMS Clerks must be designated in writing by his/her Commanding Officer. (**NOTE**: Appointment of a CMS Clerk is at the discretion of the Commanding Officer). CMS Clerks must receive training from the CMS Custodian in the physical security and administrative responsibilities associated with COMSEC material. CMS Clerks perform the following:

(1) Execute routine administrative duties and assist Custodian personnel with general file maintenance.

(2) Maintain TPI requirements after security containers containing classified keying material marked CRYPTO have been opened by Custodian personnel.

(3) Assist in conducting pagechecks and entering amendments and corrections into COMSEC and CMS -related publications.

(4) Sign receipt, inventory, and destruction reports, as a **witness only**.

(5) Assist in the placement of status markings on COMSEC material.

(6) Accompany/assist Custodian personnel in maintaining TPI when picking up COMSEC material from a CMIO or courier, and during the processing and/or transfer of COMSEC material.

b. **Restrictions**: CMS Clerks are not authorized to:

(1) Have knowledge of or access to the combinations of security containers that provide TPI.

(2) Destroy, receive, transfer or inventory COMSEC material other than in the presence of Custodian personnel.

480. CMS RESPONSIBILITIES AND DUTIES: USER PERSONNEL

a. CMS Users are responsible for the proper security, control, accountability, and disposition of all COMSEC material they handle whether or not they have signed for the material.

b. All CMS Users must complete a CMS Responsibility Acknowledgment Form (see Annex K).

c. CMS Users are responsible for the following specific duties:

(1) Comply with the applicable security, control, and accountability procedures of this manual and with all written instructions provided by Custodian personnel or higher authority.

(2) Ensure the proper inventory and destruction of COMSEC material received on local custody.

(3) Ensure that amendments to COMSEC and CMS -related publications are entered promptly and correctly.

(4) Complete, maintain, and forward required accounting records and reports to the issuing Custodian.

(5) Ensure proper storage and adequate physical security is maintained for COMSEC material.

(6) Ensure adherence to TPI requirements.

(7) Conduct training to ensure t hat all personnel handling COMSEC material are familiar with and adhere to proper CMS procedures. Document training locally in accordance with command directives.

(8) Issue COMSEC material on local custody forms after verifying that the intended recipient is authorized to hold COMSEC material and has executed a CMS Responsibility Acknowledgment Form.

(9) Report immediately to the account Custodian any known or suspected insecure practice or COMSEC incident, and follow the instructions provided by the Custodian for reporting these violations.

485. CMS RESPONSIBILITIES AND DUTIES: WITNESS

A CMS Witness is required to be familiar with the applicable procedures of this manual and related command -issued directives. An individual who witnesses an inventory, destruction, or any other CMS report is **equally** responsible for:

a. Accuracy of the information listed and the validity of the report or record used to document the transaction being witnessed.

b. Sighting all material inventoried when signing an inventory report.

c. Sighting all material to be destroyed and witnessing the actual destruction of the material.

d. Adhering to TPI requirements.

CHAPTER 5 - SAFEGUARDING COMSEC MATERIAL AND FACILITIES

501. General

505. Access and Release Requirements for COMSEC Material

a. Security Clearance
b. Requirement for Access or Need -to-Know
c. Briefing/Indoctrination
d. Written Access to COMSEC Keying Material
e. Personnel Access
f. Contractor Personnel
g. Release of COMSEC Material to a Contractor Account
h. Access to COMSEC Equipment (less CCI)
i. Displaying, Viewing, and Publicly Releasing COMSEC Material and Information
j. Release of COMSEC Material to a Foreign Government

510. Two Person Integrity (TPI) Requirements

a. Definition
b. Material Requiring TPI at the Custodian Level
c. TPI Handling and Storage Requirements at the Custod ian Level
d. Material Requiring TPI at the LH/User Level
e. TPI Handling and Storage Requirements at the LH/User Level
f. Exceptions to TPI Requirements for Electronic Key
g. COMSEC Material Completely Exempt from TPI Requirements
h. Requirement to Report TPI Violations

515. Access to and Protection of Safe Combinations

a. Selection of Combinations
b. Requirements for Changing a Combination
c. Access and Knowledge of Combinations
d. Classification of Combinations
e. Records of Combina tions
f. Sealing/Wrapping Combinations
g. Emergency Access to Containers and Combinations
h. Personal Retention of Combinations

520. Storage Requirements

a. General
b. Required Forms for Storage Containers
c. Storing Classified COMSEC Keying Material Marked CRYPTO
d. TPI Storage Containers
e. Restrictions on Use of Modified GSA Approved Security Containers and Vault Doors
f. TPI for Keyed COMSEC Equipment
g. Locking Devices
h. Storage and Protection of COMSEC Eq uipment
i. Storage of Fill Devices (FDs)
j. Storage of Other COMSEC Material

CHAPTER 5 - SAFEGUARDING COMSEC MATERIAL AND FACILITIES

525. Preparing COMSEC Material for Shipment

a. Packaging Materials/Shipment Containers
b. Wrapping Requirements
c. Wrapper Marking Requirements
d. Packaging and Shipping Restrictions

530. Transporting COMSEC Material

a. Keying Material
b. COMSEC Equipment (less CCI)
c. Other COMSEC Material
d. Commercial Aircraft
e. Courier Responsibilities
f. Restrictions on DCS Shipments
g. Airdrop of COMSEC Material
h. Electrical Transmission of Key List Settings
i. Over-the-Air Key Transfer (OTAT)
j. Over-the-Air Rekey (OTAR)

535. Controlled Cryptographic Item (CCI)

a. Definition
b. Accountability
c. General Access Requirements
d. Access Requirements for Resident Aliens
e. Access Requirements for Foreign Nationals
f. Keying CCI
g. Classification of CCI When Keyed
h. Installing CCI in a Foreign Country
i. Moving CCI to a Sensitive Environment
j. Transporting Keyed/Unkeyed CCI
k. Methods of Shipping CCI
l. Requirements and Restrictions for Transporting CCI on Commercial Aircraft
m. Storage of CCI
n. Packaging CCI
o. Notification to Intended Recipient
p. Shipments not Received
q. Reportable Incidents

540. Routine Destruction of COMSEC Material

a. General
b. Categories of COMSEC Material
c. Destruction Person nel
d. Conditions Affecting Keying Material Destruction
e. Routine Destruction of Keying Material
f. Emergency Supersession of Keying Material
g. Destruction of Maintenance Manuals, Operating Instructions, and General Doctrinal Publications

CHAPTER 5 - SAFEGUARDING COMSEC MATERIAL AND FACILITIES

CHAPTER 5 - SAFEGUARDING COMSEC MATERIAL AND FACILITIES

501. GENERAL

a. The ultimate effectiveness and protection provided by COMSEC material, systems, equipments, and techniques is dependent upon the actions of each individual user of COMSEC material.

b. All the security achieved through the proper use of cryptosystems is to a large extent dependent upon the physical protection afforded the associated keying material and those facilities where this material is stored.

c. Each person involved in the use of COMSEC material is personally responsible for:

(1) Safeguarding and properly using the material they use or for which they are responsible.

(2) Promptly reporting to proper authorities any occurrence, circumstance, or act which could jeopardize the security of COMSEC material.

d. This chapter prescribes the minimum security requirements for:

(1) Safeguarding COMSEC material to include:

(a) Access requirements.

(b) Two-Person Integrity (TPI).

(c) Access to containers or areas where COMSEC material is stored.

(d) Storage requirements.

(e) Packaging and transporting.

(f) Routine destruction.

(2) Approval and security of facilities wherein the primary purpose is telecommunications, key distribution, maintenance, and/or storage of COMSEC material.

(3) Access, storage, and transportation of COMSEC material designated as a Controlled Cryptographic Item (CCI).

e. Construction specifications for storage vaults a re contained in Annex N.

f. COMSEC facilities that hold only manual cryptosystems, unclassified keying material for machine cryptosystems, or publications other than full maintenance manuals are exempt from the facility construction requirements of this Chapter and related Annexes.

505. ACCESS AND RELEASE REQUIREMENTS FOR COMSEC MATERIAL

a. Security clearance:

Access to classified COMSEC material requires a security clearance equal to or higher than the classification of the COMSEC material involved. Access to unclassified COMSEC material does not require a security clearance. Revocation of a security clearance revokes access.

b. Requirement for Access or Need-to-Know:

Access to classified COMSEC material must be restricted to properly cleared individuals whose official duties require access to COMSEC material. The fact that an individual has a security clearance and/or holds a certain rank or position, does not, in itself, entitle an individual access to COMSEC material. Access to classified as well as unclassified COMSEC material requires a valid need-to-know.

c. Briefing/Indoctrination:

All individuals granted access to COMSEC material must be properly indoctrinated regarding the sensitivity of the material, the rules for safeguarding such material, the laws pertaining to espionage, the procedures for reporting COMSEC incidents, and the rules pertaining to foreign contacts, visits, and travel.

d. Written Access to COMSEC Keying Material:

All personnel having access to COMSEC keying material must be authorized in writing by the Commanding Officer. An individual letter or an access list may be used for this authorization.

(1) If an individual letter is used, the letter remains in effect until the status for an individual changes (i.e., a change in clearance status or duties no longer require access to COMSEC keying material).

(2) If an access list is used, it must be updated whenever the status of an individual changes or at least annually.

e. Personnel Access:

(1) U.S. Citizens:

U.S. Citizens (includes naturalized) who are U.S. Government employees, DOD contractor employees, or military personnel may be granted access to COMSEC material if they are properly cleared and their duties require access.

NOTE: Naval Reserve personnel may be granted access to COMSEC material provided they are properly cleared and are performing active duty training or assigned to drill units where access to COMSEC material is required.

(2) Resident Aliens :

Resident aliens who are U.S. Government civilian, military, or contractor personnel that have been lawfully admitted into the U.S., and have been granted a final clearance based on a background investigation, may be granted access to COMSEC material classified no higher than CONFIDENTIAL.

(a) Resident aliens withou t a security clearance may be granted access only to unclassified COMSEC keying material when their duties require such access.

(b) Resident aliens may **not** be appointed as CMS custodians, clerks, or equipment maintenance personnel nor have access to safes or areas where COMSEC keying material is stored.

(3) Foreign nationals will not be granted access to or provided information about COMSEC keying material without written permission from the material's controlling authority. Access to other COMSEC material must be approved by NSA//S11//.

(4) Security Guard Personnel :

(a) Guards whose official duties require access to COMSEC material must meet the access requirements of this chapter and be instructed concerning their responsibilities.

(b) Guards who are not given access to COMSEC material and who are used to supplement existing physical security measures, need not meet the access requirements of this chapter.

(5) Industrial Personnel :

The Commanding Officer may authorize industrial p ersonnel (e.g., naval shipyard personnel) access to classified communications spaces when required. The guidance contained in the following publications must be adhered to:

(a) NWP-4: Contains basic criteria and general access information.

(b) Cryptosystem operating instructions (KAOs): Contains specific clearance requirements for access to a cryptosystem.

(c) OPNAVINST 5510.1 (series): Contains requirements for protecting classified information.

f. Contractor Personnel :

U.S. Government COMSEC operations are normally conducted by U.S. Government personnel. However, when there is a valid need and it is clearly in the best interest of the DON and the U.S. Government, COMSEC equipment, keying material (including manual COMSEC systems), related COMSEC information, and access to classified U.S. Government information may be provided to U.S. contractor personnel to:

(1) Install, main tain, or operate COMSEC equipment for the U.S. Government.

(2) Participate in the design, planning, production, training, installation, maintenance, operation, logistical support, integration, modification, testing or study of COMSEC material or techniques.

(3) Electrically communicate classified national security information in a cryptographically secure manner or unclassified national security -related information by COMSEC protected means.

g. Release of COMSEC Material to a Contractor Account :

(1) CMS accounts that begin with "87" are civilian contractor accounts. **Before** releasing COMSEC material to a contractor account, the provisions of OPNAVINST 2221.5 (series) (Subj: Release of COMSEC Material to U.S. Industrial firms under contract to the U.S. Navy) must be met.

(2) In the event that a project/contracting officer has not fulfilled the requirements of OPNAVINST 2221.5 (series), prior to the release of COMSEC material to a contractor account, permission must be obtained from DCMS//30// by submitting the following information:

(a) Identity of Navy project office/contracting office.

(b) Contractor name and address.

(c) Contract number.

(d) Identity of COMSEC material involved.

(e) Any other information deemed appropriate in evaluating the request.

h. Access to COMSEC Equipment (less CCI):

(1) Keyed : Access to keyed COMSEC equipment requires a clearance equal to or higher than the classification of the equipment or keying material, whichever is higher.

(2) Unkeyed : Access to unkeyed COMSEC equipment may be granted to U.S. citizens whose official duties require access and who possess a security clearance equal to or higher than the classification of the equipment.

NOTE: Article 535 contains access requirements applicable to COMSEC equipment designated as CCI.

i. Displaying, Viewing, and Publicly Releasing COMSEC Material and Information :

(1) Open public display of U.S. government or foreign government COMSEC material and information at non -governmental

symposia, meetings, open houses, or for other non -official purposes is prohibited .

(a) This includes discussion, publication, or presentation for other than official purposes.

(b) No external viewing or other exposure which might afford opportunity for tampering or internal examination is permitted.

(2) Photographs, drawings, or descriptive information for press release or private use is prohibited .

(3) Exterior photographs of COMSEC equipment used for command training need not be marked "FOR OFFICIAL USE ONLY."

NOTE: FOUO markings may be removed or obscured from existing photographs.

(4) Refer requests for public or non -official display or publication of COMSEC material and information, and Freedom of Information Act (FOIA) requests to: COMNAVCOMTELCOM//N3/N32/N3X//, info DIRNSA//S5//.

(5) All contracts involving COMSEC information or material shall contain a binding non -disclosure statement to prevent the publishing of COMSEC -related information without prior approval of the contracting office.

j. Release of COMSEC Material to a Foreign Government :

Requests by foreign governments or international organizations for COMSEC material or requests to release COMSEC material to foreign governments resulting from DON operational commitments, shall be processed as follows:

(1) Submit requests with supporting data and recommendations via the chain of command to:

(a) Your command's Navy Component Commander (as listed in the Standard Navy Distribution List) if subordinate to a FLTCINC or FMF Commander; **OR**

(b) CNO//N652// or CMC//CSB// if not subordinate to a FLTCINC or FMF Commander.

(2) Provide copies of all such requests to the Navy International Program Office, Washington, D.C., and to DIRNSA FT. GEORGE G. MEADE MD//S11//.

510. TWO-PERSON INTEGRITY (TPI) REQUIREMENTS

a. Definition: TPI is a system of handling and storing designed to prevent single -person access to certain COMSEC material (identified below). (NOTE: **Non-DON personnel (e.g., Army, Air Force) are only required to adhere to national doctrine which mandates TPI handling/storage for TOP SECRET key only.)**

(1) TPI handling requires that at least two persons, authorized access to COMSEC keying material, be in constant view of each other and the COMSEC material requiring TPI whenever that material is accessed and handled. Each individual must be capable of detecting incorrect or unauthorized security procedures with respect to the task being performed.

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

NOTE: TPI storage may also be maintained by the use of a General Services Administration (GSA) procured security container or vault door eq uipped with a combination lock meeting Federal Specification FF -L-2740.

NOTE: All new security containers and vault doors procured after the effective date of this publication must be equipped with an combination lock that meets the requirements of Federal Specification FF -L-2740.

b. Material Requiring TPI at the Custodian Level :

TPI must be applied to the following COMSEC material from time of receipt through issue to LHs/users or destruction:

(1) All classified paper keying material marked or designated CRYPTO (except codes and authenticators classified SECRET and below).

(2) Fill Devices (FDs) containing classified key.

(3) Equipment containing classified key that allows for key extraction.

NOTE: When installed on the equipment and properly secured, a TPI-approved locking device/physical barrier satisfies the TPI requirement for equipment that permits extraction of its key.

c. TPI Handling and Storage Requirements at the Custodian Level:

(1) Access to and knowledge of combinations protecting TPI material at the Custodian level must be restricted to only the CMS Custodian and Alternate(s).

(2) All COMSEC material evolutions (e.g., transfer, receipt, issue to LHs/Users, destruction) conducted at the Custodian level must always be conducted by the CMS Custodian and Alternate, or the Custodian and a properly cleared person, or an Alternate and a properly -cleared person.

(3) After a container holding TPI material at the Custodian level has been opened by Custodian personnel, any properly cleared

person who has been granted access to this material may assist the CMS Custodian or Alternate in maintaining TPI and with locking the container and/or the vault.

NOTE: 1. Properly cleared non -custodian personnel are authorized to accompany the CMS Custodian or Alternate to CMIO or DCS location to receipt for and courier COMSEC material t hat requires TPI. The two individuals receipting for the material are responsible for maintaining TPI until the material is locked in a TPI container.

2. When picking up a package OTC from a CMIO or when receipting for a package from a DCS courier and there is reasonable expectation that the package contains keying material, TPI handling is required from time of pick up/receipt until the material is properly stored in a TPI container.

(4) When material requiring TPI is not being handled, it must be locked in a TPI -approved security container as specified in Article 520.

d. Material Requiring TPI at the LH/User Level :

TPI must be applied to the following COMSEC material from time of receipt through turn -in to the Custodian or Alternate, or destruction:

(1) All classified paper keying material marked or designated CRYPTO (except codes and authenticators classified SECRET and below; and GPS key).

(2) Classified electronic key whenever it is generated, transferred (OTAR/OTAT), relayed or received (OTAT). (**NOTE**: There are no TPI requirements for recipients of key received via OTAR under conditions where no FD is required at the receiving terminal.)

(3) FDs containing classified key. (**NOTE**: See TPI exceptions for COMSEC key in paragraph f.)

(4) Unloaded FDs in an operational communications environment containing keyed crypto -equipment from which classified key may be extracted.

NOTE: 1. TPI is not required if the equipment itself does not permit extraction of loaded keys (e.g., KG -66, KG -81, KG -84 A/C, KG -94, KY -57/58, KY -65/75, and KYV -5/KY -99), **OR**

2. If equipment key ports are protected against unauthorized key extraction using a TPI -approved locking device/physical barrier. In this case the unloaded FDs may be stored under single -lock protection.

(5) Equipment containing classified key which permits extraction of the key (e.g., KI -1A, KG -36).

(6) Certified key variable generator equipment (e.g., KG -83) installed for operational use. Specially designed locking bars are available for these equipments and may be used to meet TPI requirements.

KGX-93 NOTE: 1. Single-person access to the unrestricted commands is authorized.
2. Restricted commands must be accessed in accordance with TPI rules and when not manually accessed, restricted commands must be protected by the specially designed locking bar.

e. TPI Handling and Storage Requirements at the LH/User Level:

(1) Two authorized persons must be present and remain within sight of each other and the TPI material whenever it is accessed and handled. For example:

(a) Removing TPI material from COMSEC equipment.

(b) Key being generated by a key variable generator equipment (e.g., KG -83).

(c) Equipment that contains classified key which permits extraction of the key. (**NOTE**: When installed on the equipment and properly secured, a TPI -approved locking device/ physical barrier satisfies the TPI requirement.)

(2) When not in use, material requiring TPI must be protected by a TPI-approved locking device/physical barrier (in the case of equipment) or locked in a TPI storage container as specified in Article 520.

f. Exceptions To TPI Requirements for COMSEC Key:

(1) Mobile users (i.e., USMC tactical units, Naval Special Warfare (SPECWAR) units, Naval Construction Battalion units, Explosive Ordnance Disposal (EOD) units, and Mobile Inshore Undersea Warfare units (MIUWUs)) are exempt from COMSEC key TPI requirements only while operating in a tactical exercise or operational field environment.

(2) Aircraft: TPI is not required for FDs during the actual loading process in the aircraft, but TPI is required on loaded FDs up to the flight line boundary.

NOTE: 1. Loaded FDs placed in an Air Crew comm box locked with TPI approved combination locks fulfills TPI requirements. Consequently, one air crew member may transport the locked comm box up to the flight line boundary.
2. Loaded FDs may be stored onboard the aircraft in a single-lock container while the aircraft is in a flight status.

(3) Crypto Repair Facilities (CRFs), maintenance facilities, and laboratory environments are not required to maintain TPI for FDs where operational key is not handled.

(4) School/training environments using unclas key or classified key (not marked/designated CRYPTO) are not required to maintain TPI for FDs. (**NOTE**: It is, however, strongly recommended that students be taught and exercise the principles of applying TPI.)

(5) Unclassified Defense Data Network (DDN) MILNET sites are not required to maintain TPI for FDs.

(6) Users in a totally unclassified environment (e.g., data encryption standard (DES) users) are not required to maintain TPI for FDs.

(7) In facilities/spaces used solely for the storage of unkeyed equipment.

(8) Flag (e.g., FLTCINC) communicatiors operationally deployed away from their primary headquarters are exempt from TPI requirements.

g. COMSEC Material Completely Exempt From TPI Requirements :

TPI is **not required at any level** for the following COMSEC material:

(1) PROMS (programmable read -only memories).
(2) ROMS (read -only memories).
(3) MOS (metallic oxide semi -conductor) chips.
(4) Unclassified DES keying material.
(5) Maintenance key (i.e., off -the-air, in shop use).
(6) Training key not marked or designated CRYPTO.
(7) Test key (unclassified and not marked or designated CRYPTO).
(8) Repair kits.
(9) KAMs (limited or full).
(10) KAOs.
(11) MAMMs, SAMs, and SAMMs.
(12) One -time pads and tapes.
(13) Unclassified keying material (regardless of the CRYPTO markings).
(14) Unclassified, unkeyed equipment (less FDs; see TPI requirements in Article 510 f.)
(15) Unclassified equipment keyed with unclassified key.
(16) Confidential and Secret codes (regardless of CRYPTO markings).
(17) Confidential and Secret authenticators (regardless of CRYPTO markings).
(18) GPS keying material.

h. Requirement to Report TPI Violations :

Single person access to classified keying material marked or designated CRYPTO (less codes and authenticators classified SECRET and below), except when authorized in an emergency, must be reported as a COMSEC incident in accordance with Chapter 9.

515. ACCESS TO AND PROTECTION OF SAFE COMBINATIONS

a. Selection of Combinations:

Each lock must have a combination composed of randomly selected numbers based on constraints of the manufacturer. The combination must not deliberately duplicate a combination selected for another lock within the command and must not be composed of successive numbers, numbers in a systematic sequence, or predictable sequences (e.g., birthdates, social security numbers, and phone numbers).

b. Requirements for Changing a Combination:

Combinations must be changed as follows:

(1) When the lock is initially placed in use. (**NOTE:** A manufacturer preset combination may not be used.)

(2) When any person having knowledge of the combination no longer requires access (e.g., loss of clearance, transfer).

(3) When the possibility exists that the combination has been subjected to compromise (e.g., a container opened by unauthorized personnel in an emergency situation).

(4) At least annually.

c. Access and Knowledge of Combinations:

Only properly cleared and authorized individuals will have knowledge of and access to combinations protecting COMSEC material. Access and knowledge of these combinations will be restricted as follows:

(1) Custodian Vault/Safe Combinations:

Except in an emergency, the combinations to the CMS Custodian's Vault and/or safe(s) will be known only by the CMS Custodian and Alternate(s).

(2) TPI Safes/Containers:

No one person will be allowed access to or knowledge of both combinations to any one TPI container.

(3) Combinations to TPI Containers:

Except in the case of a certified locksmith, no one person may change both combinations used to maintain TPI. Neither should the same authorized individual try or verify (for the purpose of preventing a lockout) both newly changed combinations to a TPI container.

NOTE: In the case of a single Alternate only, each newly changed TPI combination shall be tried or tested only by the Custodian or Alternate authorized knowledge of or access to a particular combination. Specifically, only the Custodian or Alternate authorized access to or knowledge of combination "A" may try or test combination "A"; the same restriction applies to the "B" combination.

(4) Requirement to Report Unauthorized Access or Knowledge of Combinations to TPI Containers:

If one person gains knowledge of both combinations, except in an emergency, change both combinations, inventory the material, and submit a Loss of TPI Incident Report in accordance with Chapter 9.

(5) Changing Combinations to Containers/Vaults Protecting COMSEC material:

Combinations shall be changed only by cleared individuals who have been formally authorized access to keying material by the Commanding Officer.

NOTE: **Exception**: When properly escorted/supervised, certified locksmiths are authorized to change single -lock and TPI (double -lock) combinations when the services of a locksmith are required.

d. Classification of Combinations: Lock combinations shall be classified and safeguarded the same as the highest classification of the material being protected by the combination.

e. Records of Combinations: To provide for emergency access, a central record of the lock combinations for all COMSEC material security containers must be maintained in a security container (other than the container where CMS material is stored) approved for storage of the highest classification of the material protected by the combination locks.

f. Sealing/Wrapping Combinations: Combinations to COMSEC material security containers must be protected as follows:

(1) Each combination must be recorded and individually wrapped in aluminum foil and protectively packaged in a separate SF -700 change combination envelope.

(2) Laminate each envelope in plastic (like an identification card) or seal with plastic tape.

(3) The names and address of the individual(s) authorized access to the combinations must be recorded on the front of the envelope.

(4) Individual protectively wrapped envelopes may be stored in the same single -lock security container.

NOTE: Combinations protectively packaged in accordance with the above guidance do not require TPI handling/storage.

(5) Inspect the envelopes weekly to ensure they have not been tampered with.

g. Emergency Access to Containers and Combinations :

In an emergency, the Commanding Officer or other designated authority may direct the opening of any COMSEC material security container.

(1) At least two individuals shall be present to conduct and witness the emergency opening.

(2) After an emergency opening, the official who opened the container will make an after -the-fact report to the person in charge of the container.

(3) The individual(s) responsible for a container opened in an emergency must immediately conduct a complete inventory of the COMSEC material, and change the combinations as soon as possible.

h. Personal Retention of Combinations :

It is specifically **prohibited** for an individual to record and carry, or store insecurely for personal convenience, the combinations to COMSEC facilities or containers. Also, do not store records of such combinations in electronic form in a computer calculator or similar electronic device.

520. STORAGE REQUIREMENTS

a. General:

(1) Store COMSEC material only in containers and spaces approved for their storage. Unless COMSEC material is under the direct control of authorized persons, keep the containers and spaces locked.

(2) Comply with applicable info rmation on supplementary controls (e.g., guards and alarms) for safeguarding classified material in accordance with OPNAVINST 5510.1 (series).

(3) Store COMSEC material separately from other classified material (e.g., in separate containers or in separate drawers). This helps ensure separate control for COMSEC material and expedites emergency destruction/protection.

(4) COMSEC keying material designated for NATO use may be stored together with other COMSEC material.

(5) Unless absolutely necessary , do **not** place COMSEC material containers in commonly used passageways or other spaces where access cannot be controlled.

(6) Annex N contains construction specifications for Class A and Class B storage vaults.

b. Required Forms for Storage Containers : Storage containers for COMSEC material require the following forms:

(1) A classified container information form (Standard Form 700 (8-85)) must be placed on the inside of each COMSEC storage container.

(a) Privacy Act info rmation, (e.g., address, SSN) may be excluded from the Standard Form 700 (8 -85) and be replaced with a statement such as: "Contact OOD" command or See command recall bill," unless the individual(s) involved signed a release statement.

(b) A copy of the release statement must be maintained in the correspondence and message file.

(2) A security container open/closure log (Standard Form 702) must be maintained for each lock on a COMSEC storage container.

(3) A security container record form (OPNAV Fo rm 5510/21) must be maintained for each COMSEC storage container. This is a permanent record and must be retained with the container.

c. Storing Classified COMSEC Keying Material Marked or Designated CRYPTO :

Classified COMSEC keying material marked or designated CRYPTO must be stored as indicated below:

(1) Storage at Shore Stations :

(a) Store TOP SECRET keying material in a Class A vault **or** a GSA approved security container procured from the GSA Federal Supply Schedule.

(b) Store SECRET keying material in a Class B vault **or** in any security container approved for storing TOP SECRET keying material.

(c) Store CONFIDENTIAL keying material in a file cabinet having a built -in three -position manipulation -resistant dial -type combination lock, **or** in any storage container approved for storing SECRET **or** TOP SECRET keying material.

(2) Storage Aboard DON Ships :

(a) Store TOP SECRET keying material in a GSA approved security container with a GROUP 1 or GROUP 1R combination lock, **or** in a strong room, **or** in any storage container approved for storing TOP SECRET keying material at shore stations.

(b) Store SECRET keying material in a steel security filing cabinet having a lockbar secured with a combination padlock meeting Federal Specification FF -P-110 procured from the GSA Federal

Supply Schedule, **or** in a strong room, **or** in any storage container approved for storing SECRET or TOP SECRET keying material at shore stations.

(c) Store CONFIDENTIAL k eying material in a file cabinet secured with a combination padlock meeting Federal Specification FF -P-110, **or** in any storage container approved for storing SECRET or TOP SECRET keying material at shore stations.

(3) Storage in Mobile Situations :

TOP SECRET, SECRET and/or CONFIDENTIAL keying material may be stored in a standard, approved field safe **or** in any similar security container secured by a three -position dial -type combination padlock that meets Federal Specifications FF -P-110.

d. Two-Person Integrity Storage Containers :

(1) COMSEC material requiring TPI storage at the Custodian level must be stored within a CMS vault under one of the following options:

(a) Inside a CMS Vault equipped with one manufacturer built-in combination lock on the door, and the TPI material stored in a GSA approved container with a single or dual combination lock.

(b) Inside a CMS Vault, where the vault door is equipped with a combination lock that meets the requirements of Federal Specifications FF -L-2740. If an electromechanical lock is used, it must be programmed in either the dual combination **or** supervisory/subordinate mode for access .

(2) COMSEC material requiring TPI storage at the User level must be stored under one of the following options:

(a) In a GSA approved security container meeting Federal Specification AA -F-358G with a dual lock.

(b) In a GSA approved security container with combination lock meeting FF -L-2740.

(c) In a special access control container (SACC) securely welded to the interior of a GSA approved security container drawer.

e. Restriction on Use of Modified GSA Approved Security Containers and Vault Doors :

(1) **NO** external modifications are authorized for GSA approved security containers and vault doors after the effective date of this publication.

(2) If external modifications are made, the GSA approved security container label and the material must be removed from the

container. The container or vault door is no longer authorized for protecting **any** classified material.

(3) GSA security containers and vault doors externally modified for TPI requirements prior to the effective date of this publication may continue to be used.

NOTE: Repair and/or modification of a security container must be recorded on an associated OPNAV Form 5510/21.

(4) The available options for storing TPI material in a GSA container or vault externally modified prior to the effective date of this publication are as follows:

(a) Store COMSEC m aterial requiring TPI in a separate safe within the CMS Vault or in a SACC that has been fastened (welded to the interior of one of the drawers of the CMS safe).

(b) Install a combination lock meeting FF -L-2740 and providing dual combination capability on the door of a CMS Vault that has open storage. The following may be used in place of two built -in combination locks:

1 An approved combination padlock meeting FF -P-110 (e.g., Sargent and Greenleaf (S&G) model 8077A/8077AB) and a hardened steel hasp electrically welded to the door of the vault.

2 A steel mesh divider, with an approved combination padlock meeting FF -P-110 installed within the CMS Vault.

3 Install two combination locks or use an approved combination padlock meeting FF -P-110 with a hardened steel hasp electrically welded to the COMSEC safe(s) located outside the CMS Vault.

4 Install two approved locks on security containers used to store or hold COMSEC material requiring TPI in the CMS LH/User spaces.

f. TPI for Keyed COMSEC Equipment :

(1) TPI is required when classified keying material marked or designated CRYPTO is inserted into and extracted from COMSEC equipment and when loaded into FDs.

(2) The following methods are authorized to maintain TPI on keyed COMSEC equipment from which classified key marked or designated CRYPTO can be extracted:

(a) The continuous presence of at least two authorized persons, in sight of each other and the keyed equipment.

(b) Use of a metal cage or steel mesh divider secured with two approved locks.

(c) Installation of two approved locks on access doors to spaces where keyed COMSEC equipment is located. **(NOTE:** Cipher locks are not acceptable for this purpose; cipher locks are for personnel access control only).

(d) Installation of fabricated metal bars to the equipment racks, secured with two approved locks. The bars should traverse the card reader covers in such a manner that the bars must be removed in order to gain access to the keying material. (**NOTE**: Do not attach the bars to the equipment itself because the alteration will constitute an unauthorized modification.)

(e) Installation of a video monitoring/surveillance system in such a manner that the monitoring screen and the equipment/material can be viewed constantly.

(f) Assign additional personnel so that spaces are manned by a minimum of two properly cleared and authorized persons who are in view of each other and the material at all times.

g. Locking Devices :

The following locking devices are approved for use in establishing TPI on equipment:

(1) S&G combination padlock, model 8077A/8077AB.

(2) Standard Navy issue brass key padlocks.

(a) Each lock must be individually keyed and master keys to a series of locks are not permitted.

(b) All keys used to control access to COMSEC equipment must be strictly controlled as turn -over items on a watch -to-watch inventory. Keys cannot be removed from the spaces.

h. Storage and Protection of COMSEC Equipment :

(1) Some COMSEC equipment may, because of its configuration, require special storage facilities and procedures which are normally addressed in the handling and security doctrine for the specific system.

(2) In conjunction with any special requirements, the following guidance must be used to store and protect COMSEC equipment:

(a) Store unclassified, unkeyed equipment in a manner sufficient to preclude any reasonable chance of pilferage, theft, sabotage, tampering, or access by unauthorized persons.

(b) Store classified, unkeyed equipment in the same manner as classified material of the same classification.

NOTE: When installed in an operational configuration (e.g., in a ship, aircraft, shelter, vehicle, backpack or building), classified unkeyed COMSEC equipment may be left unattended,

provided the Commanding Officer or other responsible authority judges it is protected sufficiently to preclude any reasonable chance of pilferage, theft, sabotage, tamperin g, or access by unauthorized persons.

(c) Protect all keyed equipment based on the classification of the equipment or the keying material, whichever is higher. Additionally, ensure that procedures are in effect to prevent unauthorized use of the equipment or extraction of its key.

(3) Protect computer systems performing COMSEC functions by hardware and software controls to prevent unauthorized access and penetration. Protect machine readable copies of COMSEC programs in accordance with their classification.

i. Storage of Fill Devices (FDs):

FDs will be afforded TPI storage as follows:

(1) Custodian level storage requirements: While maintained at the custodian level (in the vault or safe of the custodian), FDs loaded with classified key marked or designated CRYPTO must be provided TPI storage. Unloaded FDs do not require TPI storage.

(2) User level storage requirements:

(a) While maintained at the user level (e.g., held by users on local custody), FDs loaded with classified key marked or designated CRYPTO must be provided TPI storage.

(b) Unloaded FDs in an operational, communications environment containing keyed equipments from which classified key marked or designated CRYPTO may be extracted must also be provided TPI storage.

j. Storage of Other COMSEC Material:

(1) Classified COMSEC material not covered above must be stored based on its classification in accordance with OPNAVINST 5510.1 (series).

(2) Unclassified COMSEC material not designated as CCI must be stored in a manner sufficient to preclude any reasonable chance of pilferage, theft, sabotage, tampering, or access by unauthorized persons.

(3) COMSEC material designated as CCI must be handled in accordance with Article 535.

525. PREPARING COMSEC MATERIAL FOR SHIPMENT

a. Packaging Materials/Shipment Containers: Materials used for packaging COMSEC material for transportation must be strong enough to protect the material while in transit, prevent items from breaking through the container, and enable detection of any tampering.

b. Wrapping Requirements :

(1) All COMSEC keying material and classified COMSEC material must be double -wrapped (using a non -transparent wrapper) and securely sealed.

(2) Unclassified COMSEC material need only be wrapped once (using a non -transparent wrapper).

c. Wrapper Marking Requirements :

(1) Inner wrapper : The inner wrapper must be marked with the following information:

(a) Highest classification of the material.
(b) "TO and "FROM" add ressees.
(c) CMS account number of both the shipping and receiving command.
(d) CRYPTO or other special handling markings.
(e) Controlled package number or registered mail number.
(f) **"TO BE OPENED ONLY BY CMS CUSTODIAN** ."

(2) Outer wrapper : The outer wrapper must be marked with the following information (applicable for shipments of all COMSEC material):

(a) "TO" and "FROM" addressees.
(b) Any applicable notation to aid delivery of the package.

NOTE: The outer wrapper mus t never reveal whether the package contains classified information or keying material (i.e., the contents of the package are not to be disclosed in any manner on the outer wrapper).

(3) The manner in how the package must be addressed may vary slightly depending on the shipment method used. Use the following guidance as applicable:

(a) When transporting material via DCS, conform to DCS guidance on packaging requirements. Further information on DCS can be obtained by contacting your servicing DCS station.

(b) Material transmitted by State Department diplomatic pouch must indicate that " **Courier Accompaniment is Required** ."

(c) When using a commercial carrier to transport CCI, a complete address must be used (this includes the street address, building number, and zip code).

NOTE: Some commercial carriers may also require the telephone number of the receiving command to be on the address label of the package.

d. Packaging and Shipping Restrictions :

(1) Package keying material separately from its associated COMSEC equipment unless the application or design of the equipment is such that the corresponding keying material cannot be physically separated from it.

(2) Ship equipment with embedded COMSEC material the same way as keying material is shipped.

(3) Package primary and associated keying material (e.g., KW-46 BAV and UV) in separate packages within a shipment.

(4) COMSEC equipment must not be shipped in a keyed condition unless removal of the keying material is impossible. (**NOTE**: For equipment using a crypto -ignition key (CIK), removal of the CIK results in the equipment being unkeyed.)

(5) When shipping keying material marked CRYPTO, packages will contain no more than four editions (for material that is superseded quarterly or more frequently) or two editions if the material is superseded semi -annually or less frequently.

NOTE: This restriction does not apply to packaged irregularly superseded keying material and may be waived by DCMS//20//when establishing a new account or in cases where supply is difficult and the number of shipments is limited.

(6) If the quantity of material to be shipped exceeds that in paragraph (5), the material must be split into several packages and entered into DCS in staggered shipments that are not likely to be combined.

(7) There is no restriction on the number of short titles that can be enclosed in each package or the number of copies of an edition.

530. TRANSPORTING COMSEC MATERIAL

The p rovisions of this article apply only to the physical movement between CMS accounts. Movements within a command may be performed by a properly cleared and autho-rized individual. The authorized methods of transporting COMSEC material are as follows:

a. Keying Material :

(1) TOP SECRET and SECRET : All TOP SECRET and SECRET keying material marked or designated CRYPTO and items that embody or describe a cryptographic logic or algorithm must be transported by one of the following methods:

(a) Defense Courier Service (DCS).

(b) State Department Courier Service (SDCS).

(c) Cleared department, agency, or contractor individuals designated as couriers. **(NOTE:** Material must be handled in accordance with TPI standards.)

NOTE: TPI is not required for keying material in the custody of the DCS or SDCS.

(2) CONFIDENTIAL : CONFIDENTIAL keying material marked or designated CRYPTO and items that embody or describe a cryptographic logic or algorithm must be transported by one of the following methods:

(a) Any method approved for TOP SECRET or SECRET.

(b) U.S. Postal Service Registered mail, provided the material does not pass through a foreign postal system, or any foreign inspection.

NOTE: Registered mail sent to FPO AE/FPO AP addresses does not pass out of U.S. control.

(c) Cleared commercial courier using Protective Security Service (PSS).

(3) UNCLASSIFIED : Unclassified keying material marked or designated CRYPTO must be transported by:

Any metho d approved for TOP SECRET, SECRET, or CONFIDENTIAL.

NOTE: 1. Under no circumstances will uncleared commercial carrier services be used to ship any keying material marked or designated CRYPTO.
2. **Never** ship **any** keying material via regular U.S. mail.

b. COMSEC Equipment (less CCI):

(1) TOP SECRET and SECRET :

(a) Any method approved for TOP SECRET or SECRET keying material.

(b) SECRET COMSEC equipment may also be shipped by a cleared commercial carrier using PSS.

(2) CONFIDENTIAL :

(a) Any method approved for TOP SECRET or SECRET.

(b) U.S. Military or military -contract air service (e.g., MAC, LOGAIR, QUICKTRANS) provided that a continuous chain of accountability and custody (e.g., signature tally record) is maintained.

(3) UNCLASSIFIED :

Unclassified equipment (not designated CCI) may be transported by any method approved for the transportation of valuable government property.

NOTE: Methods for shipping CCIs are contained in Article 535.

c. Other COMSEC Material : COMSEC material not covered above may be transported as follows:

(1) TOP SECRET material must be transported by DCS, SDCS, or cleared department, agency, or contractor courier.

(2) SECRET :

(a) U.S. Postal Service Registered mail provided the material does not pass through a foreign postal system or any foreign inspection.

(b) Cleared commercial courier using PSS.

(3) CONFIDENTIAL :

(a) U.S. Postal Service Registered mail provided the material does not pass through a foreign postal system or any foreign inspection.

(b) Commercial carrier that can provide a continuous chain of accountability and custody (e.g., signature tally record) for the material while in transit.

(4) UNCLASSIFIED :

Any means that will reasonably ensure safe and undamaged arrival at its destination.

NOTE: 1. Unclassified items may be shipped with classified items when there is an operational need to provide both types together (e.g., elements, subassemblies, and assemblies that function together and are necessary to the operation of a classified COMSEC equipment or system).
2. In the above situation, the material must be shipped in a manner approved for the highest classification of material contained in the package.

d. Commercial Aircraft :

(1) COs, OICs, or SCMSROs are authorized, in cases of operational necessity, to approve the use of commercial aircraft to transport only that quantity of COMSEC material required to fulfill immediate, operational needs, provided :

(a) Departmental and FAA Advisory Circular (AC 108 -3) procedures are followed.

(b) Couriers are briefed on their responsibilities.

(2) Direct flights should be used and unless operationally necessary, do not transport keying material in aircraft over hostile territory.

(3) U.S. flag aircraft can be used to courier COMSEC material within CONUS (includes Alaska, Hawaii, and U.S. territories/possessions).

(4) Transportation of COMSEC material outside of CONUS o n a U.S. flag or any foreign -owned, controlled, or chartered aircraft, is strongly discouraged because of the threat by terrorists and the lack of U.S. control.

e. Courier Responsibilities : Couriers shall be designated in writing and receive written instructions for safeguarding the material entrusted to them. The following provisions, at a minimum , must be adhered to:

(1) When possible, couriers must retain personal possession or control of couriered COMSEC material (e.g., material locked in an area/compartment of the aircraft and the courier has the keys to the lock or the keys are entrusted to a designated airline employee).

(a) Couriers must remain in an adjacent area to guard against unauthorized access to COMSEC material placed in a locked compartment not under their direct control.

(b) Arranging with the carrier a last -in-first -out (LIFO) procedure when the physical configuration of the conveyance does not allow the couriers to keep the material with them or under their control.

(2) Ensuring that the material is not subject to inspection by unauthorized persons when transporting COMSEC material into, within, or out of foreign countries.

NOTE: External viewing and x -raying of protectively packaged paper or mylar tape keying material is permitted, but must be done in the presence of the courier(s).

(3) When couriering COMSEC material outside of CONUS, couriers must have the telephone number of the nearest U.S. Embassy or Consulate for every country which the aircraft is scheduled to fly through/to.

(4) Notify the recipient, in advance, of the flight itinerary and estimated time of arrival so that appropriate steps may be taken if the courier does not arrive within a reasonable amount of time after the flight has arrived.

(5) Be provided specific instructions for emergency situations.

(6) Couriering of material within a command must be restricted to E-5 and above (or equivalent) personnel.

f. Restrictions on DCS Shipments :

Under DOD Dir ective 5200.33 the following types of material may be sent through the DCS:

(1) CLASSIFIED :

(a) COMSEC material.

(b) Cryptologic material.

(c) Imagery material (Secret or higher)

(2) UNCLASSIFIED :

(a)

h. Electrical Transmission of Key List Settings :

(1) The Controlling Authority (CA) of keying material may authorize secure electrical transmission of key list settings to authorized holders who cannot be supplied through normal channels.

(2) In an emergency, the CO of the transmitting station may authorize electrical transmission of key list settings to authorized holders, but must notify the CA as soon as possible thereafter.

i. Over-the-Air Key Transfer (OTAT): Net Control Stations (NCSs), Circuit Control Offices, and Operational Commanders are authorized to transmit key, which is obtained through normal channels or is locally generated, over -the-air to interconnecting stations or supporting units.

NOTE: Only established secure circuits that employ crypto systems designated for OTAT may be used.

j. Over-the-Air Rekeying (OTAR): NCSs and Circuit Control Officers are authorized to conduct OTAR with key that is obtained through normal channels or is locally generated, and rekey remote circuits under their control that employ crypto systems designated for OTAR.

NOTE: NAG 16 (series) contains procedures for conducting OTAT/OTAR of COMSEC key needed to support tactical communications.

535. CONTROLLED CRYPTOGRAPHIC ITEM (CCI)

a. Definition:

A secure telecommunications or information handling equipment, or associated cryptographic component, which is unclassified but controlled. Designated items will bear the designation Controlled Cryptographic Item or CCI.

b. Accountability:

CCI is centrally accounta ble to DCMS by serial number (AL 1) or quantity (AL 2).

c. General Access Requirements:

A security clearance is not required for access to unkeyed CCI. Normally, access must be restricted to U.S. citizens whose duties require such access.

d. Access Requirements for Resident Aliens:

Resident aliens who are U.S. Government employees, U.S. Government contractor employees, or National Guard, active duty, or reserve members of the U.S. Armed Forces may be granted access to CCI provided their duties require access.

e. Access Requirements for Foreign Nationals :

Non-U.S. citizens who are employed by the U.S. Government at foreign locations where there is a significant U.S. military presence (two or more military bases) may handle CCI material in connection with warehouse functions, provided they are under the direct supervision of an individual who has been granted access to CCI material.

(1) Access to Unkeyed CCI : Access may be granted to Foreign Nationals under the following conditions:

(a) In conjunction with building maintenance, custodial duties, or other operational responsibilities that were performed by unescorted personnel in the area prior to the installation of the CCI.

(b) The CCI is installed within U.S. controlled or combined facility with a permanent U.S. presence, as opposed to a host nation facility.

(c) Command security authority has determined that the risk of tampering with the CCI, which could result in compromise of U.S. classified or sensitive classified information, is acceptable in light of the local threat, perceived vulnerability, and the sensitivity of the information being protected as indicated by its classification, special security control, and intelligence life.

(d) The system doctrine for the CCI does not specifically prohibit such access.

(2) Access to Keyed CCI : The access requirements listed above for unkeyed CCI also apply to keyed CCI with the following additional restrictions:

(a) The non-U.S. citizens are civilian employees of the U.S. Government and are assigned to a combined facility.

(b) The non-U.S. citizens hold a clearance at least equal to the highest level of the keying material or information being processed.

(c) The CCI material remains U.S. property and a U.S. citizen is responsible for it. The presence of such installed CCIs must be verified at least monthly and the verification documented and retained in accordance with local command policy.

(d) The communications to be protected a re determined to be essential to the support of a U.S. or combined operation.

(e) U.S. users communicating with such terminals are made aware of the non-U.S. citizen status of the CCI user.

NOTE: 1. Waivers to permit unescorted access by non-U.S. citizens to installed CCIs under the conditions listed above must be submitted to DCMS//20//. (R

2. Non-U.S. citizens in communist bloc or other countries listed in the Attorney General's Criteria Country list may not be granted access to installed CCI equipment without approval from DIRNSA//S11//; submit requests via the Chain of Command to DCMS//20//. (R

f. Keying CCI:

(1) Only properly cleared and designated U.S. citizens are authorized to key CCI with classified U.S. key. Waivers of this policy must be authorized by DCMS//20//. (R

(2) Non-U.S. personnel are authorized to key CCI using only Allied key or unclassified U.S. key.

g. Classification of CCI When Keyed:

When keyed, CCI assumes the classification of the keying material it contains, and must be handled in accordance with the control and safeguarding requirements for classified keying material described in this manual.

h. Installing CCI in a Foreign Country:

When there is an operational necessity to install and operate a CCI in a foreign country at a facility which is either unmanned or manned entirely by non-U.S. citizens, the installation must be approved, in advance, by DCMS//20//. (R

(1) In addition to the requirements listed above, special security measures will be required (e.g., constructing vault areas, storing CCI material in approved security containers, installing locking bars on equipment racks, installing alarm systems) to prevent unauthorized access to the CCI by non-U.S. citizens.

(2) The installation of the CCI must be accomplished and controlled by U.S. citizens.

i. Moving CCI to a Sensitive Environment. CCI material should not be moved from an environment where the risk of tampering by non-U.S. citizens is acceptable, to a more sensitive environment where the risk of tampering by non-U.S. citizens is not acceptable.

(1) When operational requirements necessitate moving CCI to a more sensitive environment, the command must send a message to DCMS//20// requesting authorization to move the material. (R

(2) Before moving the CCI, it must be examined for signs of tampering by qualified COMSEC maintenance personnel.

(3) Report any evidence or suspicion of tampering to DIRNSA//V51A// as a COMSEC incident in accordance with Chapter 9. (R

NOTE: If tampering is suspected, remove the CCI from operational use until instructions are received from DIRNSA.

j. Transporting Keyed/Unkeyed CCI :

(1) CCI must not be shipped in a keyed condition unless removing the key is impossible.

(2) Unkeyed CCI may be shipped/transported by any means delineated below.

k. Methods of Shipping CCI . CCI equipment must be shipped only to authorized activities using any of the following methods:

(1) Authorized U.S. Government department, service, or agency courier (e.g., Navy Supply System).

(2) Authorized U.S. Government Contractor/Company or U.S. citizen courier.

(3) U.S. Postal Service Registered mail, provided the material does not at any time pass out of U.S. postal control, pass through a foreign postal system, pass through any foreign inspection, or otherwise fall under the control of unescorted foreign nationals.

NOTE: 1. There are certain restrictions gov erning the size and weight of packages that can be shipped via registered mail. Prior to shipping the CCI, check with the postal service to determine whether the shipment qualifies.
2. First, fourth, certified, insured, and express mail, and parcel post are **not** authorized methods of shipping CCI equipment.

(4) Commercial carriers (non -military aircraft) may be used to transport CCI (includes CCI being transported in conjunction with Foreign Military Sales) within the U.S., its territories, and possessions, providing the carrier warrants in writing to satisfy the following:

(a) Is a firm incorporated in the U.S. that provides door -to -door service.

(b) Guarantees delivery within a reasonable number of days based on the distance to be traveled.

(c) Possesses a means of tracking individual packages within its system to the extent that should a package become lost, the carrier can, within 24 hours following notification, provide information regarding the last known location of the package(s).

(d) Guarantees the integrity of the vehicle's contents at all times.

(e) Guarantees that the package will be stored in a security cage should it become necessary for the carrier to make a prolonged stop at a carrier terminal.

(f) Utilizes a signature/tally record (e.g., a carrier's local signature/tally form or the DD Form 1907 or Form AC-10) that accurately reflects a continuous chain of accountability and custody by each individual who assumes responsibility for the shipment while it is in transit; **OR**

1 Utilizes an electronic tracking system that reflects a chain of accountability and custody similar to that provided by a manually prepared signature/tally record.

2 Ensures positive identification of the actual recipient of the material at the final destination.

3 Uses a hard -copy printout that serves as proof of service; the printout must reflect those points, during transit, where electronic tracking of the package/shipment occurred.

(5) U.S. military, military -contractor, or private air service (e.g., AMC, LOGAIR, QUICKTRANS), provided the carrier (R satisfies the requirements identified above for commercial non-aircraft carriers.

(6) U.S. Diplomatic Courier Service.

(7) DCS outside CONUS, when no other method of secure transportation is available.

(8) Commercial passenger aircraft may be used within the U. S., its territories, and possessions. (**NOTE**: Commercial passenger aircraft used outside the U.S., its territories, and possessions must be a U.S. flag carrier.

(NOTE: Requirements/restrictions for shipping CCI on commercial aircraft are detailed in paragraph l.)

(9) Non-U.S. citizens who are employed by the U.S. Government at foreign locations where there is a significant U.S. military presence (two or more military bases) may transport CCI material, provided there is a signature record that provides continuous accountability for custody of the shipment from the time of pick -up to arrival a t the final destination.

NOTE: A U.S. citizen must accompany the foreign driver in couriering the material; or the material must be contained in a closed vehicle or shipping container (e.g., CONEX, DROMEDARY, or similar authorized container) which is locked with a high security lock and contains a shipping seal that will prevent undetected access to the enclosed material.

l. Requirements and Restrictions for Transporting CCI on Commercial Aircraft:

(1) The container(s) and content(s) may be subject to certain security inspections, including x -ray, by airport personnel. Inspections are permissible, but only in the presence of the courier.

(2) Inspection of CCI material must be restricted to exterior examination only and conducted in the presence of the courier. To preclude unnecessary inspections by airport personnel, couriers should carry current orders, letters, and ID cards identifying them as designated couriers.

(3) CCI material must be stored in the cabin of the aircraft where the courier can maintain continuous control of the material.

(4) When the size of the CCI shipment is too large for storage in the cabin of the aircraft, the entire shipment must be packaged in a suitable container which is secured and sealed in such a manner so that any unauthorized access to the enclosed CCI can be detected by the courier. (**NOTE:** The CCI shipment may then be shipped as checked baggage, provided the LIFO procedure is coordinated with the carrier.)

m. Storage of CCI: Unkeyed CCI and/or CCI keyed with unclassified key marked or designated CRYPTO, must be stored in a manner that affords protection against pilferage, theft, sabotage, or tampering, and ensures that access and accounting integrity are maintained.

n. Packaging CCI: Package unkeyed CCI for shipment in a manner that will allow for tamper detection and prevent damage while in transit.

(1) In addition to the information required on the packaging label, include the office code or duty position title of the individual who is designated to accept custody of the CCI equipment to ensure proper delivery. (**NOTE**: Do not use the name of an individual.)

(2) The shipping document must also contain an emergency telephone number(s) for the intended recipient in the event delivery is made after normal working hours.

o. Notification to Intended Recipient. Regardless of the method used to transport CCI, the transferring command must, within 24 hours of shipping, notify the intended recipient of the method of transportation and a list of CCI(s) that have been shipped.

p. Shipments not Received:

(1) If a shipment of CCI equipment has not been received within five working days after the expected delivery date, contact the originator of the shipment immediately.

(2) If the location of the shipment cannot be determined, tracer action must then be initiated. The material shall be assumed to be lost and the incident must be reported to DIRNSA FT GEORGE G MEADE MD//V51A// in accordance with Chapter 9. (R

q. Reportable Incidents: (R

(1) Lost shipments, shipments that show evidence of possible tampering, and unauthorized access to CCI equipment must be reported to DIRNSA//V51A//, info DCMS//20//.

(2) All other incidents involving improper shipping or handling of CCI equipment must be reported to DCMS//20//, info DIRNSA//V51A//. If a commercial carrier is involved, include the name(s) of the carrier(s). (R

540. ROUTINE DESTRUCTION OF COMSEC MATERIAL

a. General. Effective and superseded keying material is extremely sensitive, and if compromised, potentially exposes to compromise all of the information encrypted by it. For this reason, keying material (other than defective or faulty key) must be destroyed as soon as possible after it has been superseded or has otherwise served its intended purpose.

NOTE: Failure to destroy COMSEC material within the timeframes outlined in this article is a locally reporta ble PDS in accordance with Chapter 10. Do not report late destructions to DCMS.

b. Categories of COMSEC Material. The various categories of COMSEC material that are discussed below are detailed in Article 260 and should be reviewed as often as necessary to ensure compliance with the destruction requirements contained in this chapter.

c. Destruction Personnel. COMSEC material that is authorized for destruction must always be destroyed by two cleared and authorized personnel in accordance with the following:

(1) Unissued (i.e., retained in the vault or safe of the Custodian) superseded COMSEC material must be destroyed by custodian personnel, or by the Custodian or Alternate and a properly cleared witness.

(2) Issued (i.e., to a LH/User for use) superseded COMSEC material must be destroyed by any two properly cleared and authorized personnel.

d. Conditions Affecting Keying Material Destruction: The destruction requirements for keying material will vary depending on several factors; for example:

(1) Whether or not the keying material is marked or designated CRYPTO,

(2) Whether it has been issued to Users, or,

(3) Whether it remains unissued (i.e., in the Custodian or LH Vault or safe), etc. Accordingly, these factors and how they affect the 12 -hour standard are identified in the Routine Destruction and Emergency Supersession exceptions stated in paragraphs e. and f.

e. Routine Destruction of Keying Material (both regularly and irregularly superseded). Destroy immediately after use when more than one copy of the key setting is available, or as soon as possible after the cryptoperiod and always within 12 hours after the end of the cryptoperiod. **Exceptions** to the 12 -hour destruction standard are as follows:

(1) In the case of an extended holiday period (over 72 hours) or when special circumstances prevent compliance with the 12-hour standard (e.g., destruction facility or operational space not occupied) destruction may be extended until the next duty day. In such cases, the material must be destroyed as soon as possible after reporting for duty.

(2) Superseded keying material on board an aircraft is exempt from the 12 -hour destruction standard. However, superseded keying material must be destroyed as soon as practicable upon completion of airborne operations.

(3) Superseded segments of sealed segmented/ extractable keying material (issued or unissued), need not be destroyed until the entire edition is superseded or the keying material is unsealed, whichever occurs first. When retained until the entire edition is superseded, the material must be destroyed no later than 5 working days after the month in which supersession occurs.

NOTE: "Sealed" keying material is defined as that which either remains unopened in its original protective packaging or which has been resealed in accordance with Article 772. Canister -packaged keying material is considered sealed, even after initial use (one or more segments have been removed from the canister for use). Accordingly, superseded segments need not be removed and destroyed until an effective segment is required for use or until the entire edition is superseded, whichever occurs first.

(4) Issued keying material packaged in canisters containing multiple copies of each segment (e.g., 1/01, 1/02, 1/03, etc.):

(a) Destroy all copies except the last copy immediately after use.

(b) Retain the last copy of each effective segment until the cryptoperiod expires, then destroy within 12 hours.

(5) Issued codes (e.g., AKAC 874) consisting of sections that are used incrementally (e.g., 6-hour periods). Destruction of each 6-hour section need not be carried out until the entire table or page is superseded. Users then have 12 hours from the time the entire table or page supersedes to complete destruction.

(6) Keying material that supersedes at intervals of less than one month (e.g., 7-, 10-, and 15-day codes):

(a) Unissued: The keying material may be held until the next end of the month destruction, but must be destroyed no later than five working days after the end of the month in which the edition was superseded.

(b) Issued: CMS Users need not open security containers for the sole purpose of performing routine destruction. However, if the security containers are opened for any reason and Users have access to the material, the superseded material must be destroyed.

(7) Irregularly superseded keying material whose supersession is promulgated by message must be destroyed as follows:

(a) Unissued: The keying material may be held until the end of the month destruction, but must be destroyed no later than five working days after the month in which supersession occurs.

(b) Issued: Destroy as soon as possible after receipt of the supersession message and always within 12 hours of receipt of the message.

(8) Superseded COMSEC material received in an ROB shipment must be destroyed as soon as possible but always within 12 hours of opening the shipment. Annotate on the SF 153 destruction document, "SUPERSEDED ON RECEIPT." No additional reporting is required.

(9) Destroy irregularly superseded training/maintenance keying material when it becomes physically unserviceable.

(10) Destroy on-the-air test key at the end of the testing period as determined by the test director.

(11) If material is involved in an investigation, specific instructions to retain the material beyond its supersession date will be provided by DCMS//20//.

(12) To permit processing of message traffic received after the effective cryptoperiod of a key, keying material for all automanual off-line systems (e.g., KL-42, KL-43, KL-51) may be retained up to, but no longer than, 72 hours after supersession.

f. Emergency Supersession of Keying Material. When involved in compromise situations, destroy superseded material as soon as possible and always within 12 hours of receipt of emergency supersession notification. The only exceptions to this 12-hour destruction standard are as follows:

(1) In the case of an extended holiday period (over 72 hours) or when special circumstances prevent compliance with the 12-hour standard, destruction may be delayed until the next duty day. In such cases, destruction must be conducted as soon as possible after reporting for duty.

(2) When a segment of issued canister-packaged keying material is emergency superseded before its cryptoperiod, comply with the following:

(a) Do not remove the emergency superseded segment from the canister for destruction until all segments preceding the superseded segment have been used or destroyed.

(b) Until such time as the emergency superseded segment(s) can be removed from the canister for destruction, adhere to the following procedures to prevent accidental use of the superseded segment:

1 Place the affected canister in a ziplock bag along with a copy of the message directing emergency supersession of the segment(s), **OR**

2 Wrap a copy of the supersession message securely around the canister using a rubber band.

(c) When a segment of unissued canister-packaged keying material, is emergency superseded before its cryptoperiod, comply with the following:

1 Follow the procedures described above for issued canister-packaged keying material or hold the unissued canister for routine end of the month destruction.

2 When held until the end of the month, the Custodian must ensure that the keying material is destroyed no later than five working days after the month in which supersession of the entire edition occurs.

(3) When unissued keying material protectively packaged in other than canisters is emergency superseded, comply with the following:

(a) Destroy superseded segments immediately or hold the unissued keying material edition for routine end of month destruction.

(b) To prevent accidental use of superseded segments, wrap/attach a copy of the supersession message securely (e.g., using a rubber band) around the remainder of the material.

(c) When held until the end of the month, the Custodian will ensure that the keying material is destroyed no later than five working days following supersession of the entire edition.

g. Destruction of Maintenance Manuals, Operating Instructions, and General Doctrinal Publications :

(1) Destroy within five working days after the end of the month in which superseded.

(2) Residue of classified amendments to these publications must be destroyed as soon as possible, but no later than five working days after entry of the amendment.

(3) Residue of unclassified amendments to the publications must be destroyed as soon as possible, but no later than five working days after the end of the month in which the amendment was entered.

h. Destruction of COMSEC Equipment . Unless otherwise directed by DCMS//30//, COMSEC equipment will **NOT** be destroyed at the local command level, but will be disposed of as directed by DCMS. The following guidance pertains:

(1) When authorization to destroy COMSEC equipment has been received by an account from DCMS//30// and a deadline destruction date has not been identified:

(a) Destroy within 90 days of receipt of the destruction authorization. If destruction cannot be accomplished within this specified timeframe, the account must request a waiver from DCMS//20/30// identifying material involved; authorization message date-time-group; circumstances as to why the account can not comply; and anticipated date of destruction.

(b) Accounts that fail to destroy material within the 90 day timeframe and who have not requested a waiver are in violation of CMS policy and must document "late destruction" in accordance with Art. 1005.a.(5).

(2) COMSEC equipment can not be destroyed until all users on that particular net are up and operational. Therefore, accounts must exercise caution to ensure no degradation in communications when changing from one secure system to another.

(3) COMSEC equipment identified for destruction will remain on an accounts inventory until actual destruction and reporting has been documented.

(4) Questions concerning COMSEC equipment destruction, other than that indicated, may be referred to DCMS//30//.

i. Reporting Destruction. Report destruction in accordance with the guidance contained in Chapter 7 or as directed by DCMS.

j. Routine Destruction Methods:

(1) Paper COMSEC Material : Destroy paper COMSEC material by burning, crosscut (double-cut) shredding, pulping, chopping or pulverizing.

(a) When burning, the combustion must be complete so all material is reduced to white ash and contained so that no unburned pieces escape. Inspect ashes and break up or reduce to a sludge if necessary.

(b) Placing superseded keying material in a burn bag does not constitute a complete destruction. A complete destruction is the actual destruction by burning, shredding, or other authorized means that makes recovery or reproduction impossible.

(c) Do not transport burn bags of unshredded COMSEC keying material to destruction facilities outside the jurisdiction of the command unless controlled by the Custodian and/or Alternate and a qualified witness.

(d) Pulping (wet process) devices, or chopping or pulverizing (dry process) devices must reduce the residue to bits no larger than five millimeters (5mm) in any dimension. A good quality multi-speed household blender may be used.

(e) Crosscut shredders must reduce the r esidue to shreds no more than 3/64-inch (1.2mm) by 1/2-inch (13mm) or 1/35-inch (0.73mm) by 7/8-inch (22.2mm).

(f) When destroying small amounts of keying material (i.e., keytape segments or key cards), add an equal amount of other classified or unclassified material of similar composition before shredding.

(g) Normally, strip-shredding is not an approved destruction method, but ships and submarines may use strip-shredders that cut the material into strips no wider than 1/32 inch in the following instances.

1 Ships at sea and surfaced submarines without incinerators may use strip-shredders. Stream the strip-shredded material loosely into the wake of the ship in open water when the CO considers recovery by hostile forces unlikely.

2 Ships or submarines in port must burn strip-shredded material; however they may temporarily retain strip-shredded material (for no longer than seven days) for streaming in the wake of the ship upon return to sea.

3 Submerged submarines with hydraulic compactors shall compress the shredded material into a standard disposable perforated metal container; ensure the container weighs at least 30 pounds, seal at both ends, and jettison from the trash disposal unit in a least 1,000 fathoms of water.

NOTE: On board ships, submarines, and aircraft superseded keying material may be shredded and kept in secure storage (for no longer than seven days) until a facility is reached where complete destruction can be accomplished.

(2) Non-paper COMSEC Material . Destroy by burning, chopping, pulverizing, or chemically altering, until it is decomposed to such a degree that there is no possibility of reconstructing key, keying logic, or classified COMSEC information by physical, electrical, optical or other means.

(a) Microfiche may be destroyed by burning or by using an NSA-approved COMSEC microfiche and microfilm shredder. Before burning, put each microfiche in a separate paper jacket. If needed, add shredded or crumpled paper before burning.

(b) Use acetone or methylene chloride to destroy microfiche when burning is not feasible. Enclose each microfiche in a separate paper jacket or place in the chemical bath one at a time.

W A R N I N G: **Use acetone carefully; it is volatile, toxic, and flammable. Avoid spark or flame and wear gloves, aprons, and eye protection. Consult the local safety officer for additional precautions.**

1 Submarines in port shall destroy microfiche by one of the approved methods above.

2 Submarines at sea may destroy microfiche by strip-shredding it and jettisoning the residue with the COMSEC paper residue as stated above, or may retain the microfiche until return to port and then destroy it using an approved method.

(c) Magnetic or electronic storage/recording media are handled on an individual basis. Destroy magnetic tapes by disintegration incineration and magnetic cores by incineration or smelting. Destroy magnetic disks and disc packs by removing the entire recording surface by means of an emery wheel or sander.

W A R N I N G: **Do NOT burn magnetic tape on aluminum reels in a sodium nitrate fire (this may cause an explosion).**

(d) Puncture empty keytape canisters on both sides of the canister and dispose of it as unclassified material. Ensure that the canister is empty before disposing of it.

(e) Equipment must be destroyed as specifically directed by DCMS//30//.

545. COMSEC FACILITIES

a. Introduction. COMSEC facilities include different types of secure telecommunications facilities and other facilities in which classified COMSEC material is contained.

b. Types of COMSEC Facilities:

(1) Fixed.

(2) Special-Purpose which includes:

(a) Unattended fixed secure telecommunications facilities.

(b) Contingency fixed secure telecommunications facilities.

(c) Fixed secure subscriber facilities.

(3) Transportable and Mobile.

(4) DOD Black Bulk Facility.

c. Construction Requirements. The different types of facilities are grouped into categories and their minimum construction requirements are delineated in Annexes O and P. Maximum physical security, however, is achieved when COMSEC facilities are constructed in accordance with the vault-type construction requirements in Annex N.

550. SAFEGUARDING FIXED COMSEC FACILITIES.

a. Location. Locate a fixed COMSEC facility in an area which provides positive control over access, and as far as possible from areas which are difficult or impossible to control (e.g., parking lots, ground floor exterior walls, multiple corridors or driveways, or surrounded by other uncontrolled buildings or offices).

b. Construction Requirements. See Annex O.

c. Installation Criteria. Facilities that generate, process, or transfer unencrypted classified information by electrical, electronic, electromechanical, or optical means shall

conform to the guidance and standards herein and OPNAVINST C5510.93 (series) (Navy Implementation of National Policy on Control of Compromising Emanations).

d. Facility Approvals, Inspections, and Tests :

(1) Approval to hold classified COMSEC material . Each facility must be approved by the responsible department or agency (e.g., ISIC) to hold classified COMSEC material prior to its use.

(a) This approval should be based upon a physical security inspection that determines whether or not the facility meets the physical safeguarding standards of this chapter and Annex O.

(b) After initial appro val, the facility will be reinspected at intervals no greater than 24 months.

(c) The facility shall also be reinspected, and approval confirmed, when there is evidence of penetration or tampering, after alterations that significantly change the physical characteristics of the facility, when the facility is relocated, or when it is reoccupied after being temporarily abandoned.

NOTE: When needed, consult the Security Manager and/or the CMS Custodian for advice about inspections. (R

(2) Approval to Operate Secure Telecommunications Facilities and Key Distribution Centers :

(a) General COMSEC Inspection . In addition to the physical security inspection above, conduct a general COMSEC inspection prior to initial activation, where practicable, but in no case later than 90 days after activations. Thereafter, reinspection is required at intervals as stated in OPNAVINST 5040.7 (series) Subj: Naval Command Inspection Program.

(b) Technical Surveillance Countermeasures (TSCM) Inspection . Prior to initial activation, a TSCM inspection or survey must be conducted.

(3) Daily Security Check :

(a) In a continuously manned facility, make a security check at least once every 24 hours to ensure that all classified COMSEC information is properly safeguarded, and that physical security protection system/devices (e.g., door locks and vent covers) are functioning properly.

(b) In a non-continuously manned facility, conduct a security check prior to departure of the last person to ensure the facility entrance door is locked and, where installed, Intrusion Detection Systems (IDS) are activated.

(c) Where a facility is unmanned for periods greater than 24 hours (e.g., during weekends and holidays), and the facility is not protected by an approved IDS:

1 Ensure that a check is conducted at least once every 24 hours to ensure that all doors to the facility are locked, and

2 There have been no attempts at forceful entry.

(4) Quadrant Inspections . A quadrant inspection is designed to detect attempts at technical exploitation of COMSEC equipment by tampering, bugging, key extraction, or reverse engineering. If any of these conditions are known or believed to have taken place, contact DCMS//20// for additional guidance.

NOTE: Document miscellaneous inspections (e.g., daily security checks, security check after reoccupying a building that was abandoned temporarily) locally in accordance with command directives.

e. Access Restrictions and Controls :

(1) Escorted and Unescorted Access :

(a) Limit unescorted access to individuals whose duties require such access, and who meet the access requirements of Article 505 and 535.

(b) Enter the names of persons having regular duty assignments in the facility on a formal access list.

(c) The responsible authority may grant access to cleared and uncleared visitors, provided they require such access. Uncleared visitors must be continuously escorted by a properly cleared person whose name is on the access list.

NOTE: When uncleared repairmen are admitted to perform maintenance on commercially contracted information processing equipment connected to circuits protected by cryptographic equipment, the escort shall be a CRYPTO-repair person or other technically qualified person.

(d) Record all visits in the visitor register and retain the register for at least one year.

(R

(2) No-Lone Zone (NLZ) . Facilities that produce or generate key (e.g., key distribution centers) and CMIO Norfolk shall employ NLZ restrictions within all areas in which these activities take place.

(a) Facilities charged with providing or supporting essential, critical, intelligence, or command and control activities should also implement NLZ restrictions.

(b) In addition, departments and agencies may require NLZ restrictions in facilities engaged in the design, development, manufacture or maintenance of crypto equipment.

(3) Firearms. The CO or responsible civilian official shall determine the need for firearms to protect a facility as stated in department and agency directives.

f. Storage of COMSEC Material. Store COMSEC material in accordance with Articles 520 and 535.

g. Protection of Unattended COMSEC Equipment:

(1) In a non-continuously manned facility, protect unattended COMSEC equipment in accordance with Article 520 and/or 535 during periods when the facility is not manned.

(2) A facility that meets the construction requirements of Annex O provides sufficient protection, under normal circumstances, for unattended, unkeyed COMSEC equipment installed in an operational configuration.

NOTE: Requirements for the protection of COMSEC equipment in facilities which normally operate unmanned for extended periods of time are delineated in Article 555.

h. Protection of Lock Combinations. The requirements for protection of lock combinations to security containers in Article 515 apply to all COMSEC facility doors.

i. Standard Operating Procedures (SOPs). Each facility shall have a written SOP. Ensure the SOP contains provisions for securely conducting facility operations and for safeguarding COMSEC material. Additionally, each facility shall have an Emergency Action Plan (EAP) in accordance with Annex M.

j. Non-essential Audio/Visual Equipment:

(1) Personally-owned receiving, transmitting, recording, amplifying, information-processing, and photographic equipment (e.g., radios, tape records, stereos, televisions, cameras, magnetic tape and film) shall not be permitted in secure telecommunications facilities or key distribution centers.

(2) Government-owned leased (or company-owned) or leased in the case of contractor-operated facilities receiving, transmitting, recording, amplifying, video, and photographic equipment (e.g., radios, music systems, TV monitors/cameras, and

amplifiers) which are not directly associated with secure telecommunications operations or information processing activities may be used in facilities, but must be approved in writing by the Commanding Officer, and must meet the requirements of OPNAVINST C5510.93 (series).

NOTE: Medically approved health-related equipment (e.g., pacemakers and hearing aids) are exempt from this restriction, upon approval of the CO.

555. SAFEGUARDING UNATTENDED FIXED SECURE TELECOMMUNICATIONS FACILITIES.

An unattended fixed secure telecommunications facility is an operational facility in which secure telecommunications functions are performed with no operator personnel present. Such a facility normally, but not exclusively, performs a communications relay or other similar switching function. The following particulars are applicable:

a. Location. Locate these facilities in areas firmly under U.S. or Allied control, where sufficient U.S. or Allied military or police forces are located in the vicinity to provide reasonable protection against unauthorized occupation of the site.

b. Construction Requirements. Construct these facilities in accordance with Annex O. Additionally, newly constructed facilities shall have only one door and no windows.

c. Installation Criteria. Comply with guidance in Article 550.c.

d. Facility Approvals, Inspections, and Tests. In addition to the guidance listed in Article 550, inspect unattended facilities at approximately 30-day intervals to confirm the integrity of the facility.

e. Access Restrictions and Controls. Article 550.e. applies. Additionally, all persons who visit the facility, including those on the official access list, shall record each visit in the visitor register.

(1) Protect each facility with an approved IDS or protect it with guard(s). The IDS must provide for immediate guard response (i.e., arrival on-the-scene should be within five minutes).

(2) If the guard response to an alarm will be excessive, select crypto equipment for use at the facility that employs a system for remote zeroization.

f. Storage and Protection of COMSEC Material:

(1) Only operational crypto e quipment and currently effective key held in that equipment shall be permitted at an unattended facility.

(2) Do not store future key (ROB), non-operational or spare crypto equipment, or COMSEC publications (e.g., maintenance manuals or operating instructions).

(3) Install operational crypto equipment in NSA-approved containers, or use supplementary controls (e.g., locking bars to secure the equipment or an approved IDS).

NOTE: DIRNSA-approved security containers for op erational crypto equipment only are available. These containers are not approved by GSA, however, because they have holes drilled in them for cabling and ventilation.

g. Protection of Lock Combinations. Protect combinations in accordance with Article 515. Additionally, do not store records of lock combinations at an unattended facility.

h. Firearms. Article 550.e.(3) applies for guards or for other personnel who may visit the facility.

i. SOP. See Article 550.i.

j. Non-essential Audio/Visual Equipment. Comply with Article 550.j.

k. Additional Security Requirements. Personnel who visit an unattended facility to key the equipment or perform maintenance, must inspect the facility for signs of tampering or attempted penetration.

560. SAFEGUARDING CONTINGENCY FIXED SECURE TELECOMMUNICATIONS FACILITIES

a. General:

(1) These facilities contain secure telecommunications equipment in an operational configuration for rapid activation as a fully operational facility should the need arise.

(2) They may be fully equipped, or they may be partially equipped and made ready for secure communications at the time of activation.

(3) They are normally unattended, or are attended only on a part-time basis.

b. Location. Article 550 applies.

c. Construction Requirements. See Annex O.

d. Installation Criteria. Article 550.c. applies.

e. Facility Approvals, Inspections, and Tests. Comply with Article 550. Additionally, inspect these facilities at approximately 30-day intervals to confirm the integrity of the facility and to remove any superseded or extraneous material.

f. Access Restrictions and Controls. Article 550 applies. Additionally, these facilities shall have either an approved IDS or shall be guarded.

g. Storage of COMSEC Material. Store COMSEC material in accordance with Article 520 and/or 535.

h. Protection of COMSEC Equipment. Where the facility is not contained in a vault constructed as stated in Annex N, install all crypto equipment in DIRNSA-approved security containers for storage of operational crypto equipment, or use supplementary controls (e.g., locking bars to secure the equipment or an approved IDS).

i. Protection of Lock Combinations. Protect lock combinations in accordance with Article 515. Additionally, do not store records of lock combinations at unattended contingency facilities.

j. Firearms. See Article 550.e.(3).

k. SOP. See Article 550.i.

l. Non-essential Audio/Visual Equipment. See Article 550.j.

m. Additional Security Requirements. Personnel who visit a contingency facility during periods when it is unattended shall inspect the facility for signs of tampering or attempted penetration.

565. SAFEGUARDING FIXED SECURE SUBSCRIBER TELECOMMUNICATIONS FACILITIES

a. General:

(1) A fixed secure subscriber telecommunications facility is a structure, or area within a structure, in which user-operated secure voice, data, facsimile, or video circuits terminate.

NOTE: An office in which a STU-III is installed is not a Secure Subscriber Telecommunications Facility.

(2) Although these facilities are often inherently difficult to control, sufficient controls must be provided to prevent unauthorized persons from using the terminal equipment and to protect the associated crypto equipment and keying material.

b. Location. See Article 550. Additionally, locate the facility within the building proper (i.e., not on balconies, porches, bays, or other architectural projections that are not of substantial construction). Also, locate the terminal equipment in an area away from heavy pedestrian traffic.

c. Construction Requirements. A fixed secure subscriber facility ideally should be located in an area conforming to the construction requirements of Annex O. Where this is not practicable (i.e., general office spaces and residences), rigidly apply the applicable requirements which follow.

d. Access Restrictions and Controls. Limit unescorted access to the crypto equipment and associated COMSEC material to individuals who require such access and who meet the access requirements of Article 505 and/or 535.

(1) Limit unescorted use of the terminal equipment for secure communications to appropriately cleared individuals.

(2) Uncleared individuals, or persons not appropriately cleared, may use the terminal equipment for secure communications provided they are escorted by an individual who has unescorted access, and the distant end is first notified of the clearance limitations.

(3) In general office environments and in private residences where individuals work, reside, or visit, take precautions to ensure that classified conversations are not overheard by unauthorized persons and that classified messages are not left unattended.

e. Storage of COMSEC Material. Store COMSEC material in accordance with Article 520 and/or 535. Facilities other than those in private residences may hold only the current edition of keying material and operating instructions for the crypto equipment, but no other supporting COMSEC material.

(1) Facilities in private residences may hold no more than a seven-day supply of keying material (except where the key is packaged in a protective canister, then, the current edition may be held).

(2) Facilities in private residences may hold no other supporting COMSEC material.

f. Protection of Unattended COMSEC Equipment. Protect unattended crypto equipment to a degree which, in the judgment of the responsible official, is sufficient to preclude any reasonable chance of pilferage, theft, sabotage, tampering, or access by unauthorized personnel.

(1) When possible, install the crypto equipment in a DIRNSA-approved security container for storage of operational crypto equipment. Alternatively, protect the equipment by an approved IDS, or by a security force.

(2) Whenever the facility is vacated by all appropriately cleared personnel, unkey the equipment and securely store the keying material.

(3) For facilities in private residences and other unprotected areas or facilities (when the user is absent for a period of more than 72 hours), remove and securely store all classified components of the system.

570. SAFEGUARDING TRANSPORTABLE AND MOBILE COMSEC FACILITIES

a. General. The safeguards contained in this article are primarily applicable to transportable and mobile secure telecommunications facilities, but they also apply to any other transportable or mobile facility that contains classified COMSEC material (e.g., a transportable crypto-maintenance facility or a transportable or mobile key distribution center (KDC)).

b. Location. These facilities may be located wherever operational requirements dictate.

c. Construction Requirements are not prescribed for these facilities because of the many possible operational requirements which such facilities must fulfill.

d. Installation Criteria. Article 550.c. applies.

e. Facility Approvals, Inspections, and Tests:

(1) Approval as stated in Article 550 is genera lly not required. The only inspection requirement is for a daily security check.

(2) If a transportable or mobile facility remains operational in a fixed location for a period of six months or longer, consider it a fixed facility. Consequently, a facility approval, inspection, and test must be conducted in accordance with Article 550.

(3) If a transportable or mobile facility processes especially sensitive information or frequently operates where a known hostile intelligence threat exists, the requirements for TEMPEST inspections apply.

f. Access Restrictions. Article 505 and/or 535 applies, except on-duty uncleared crewmembers (e.g., in aircraft and tanks) do not require a continuous escort by an individual who has unescorted access.

NOTE: Transportable and mobile facilities employed principally to perform a telecommunications or key distribution function (e.g., a communications van or mobile KDC) shall maintain access lists and visitor registers.

g. Storage of COMSEC Material. Store COMSEC material in accordance with Article 520 and/or 535 and comply with the following additional requirements:

(1) Securely affix security containers to the facility with bolts, welds, or other appropriate means.

(2) Limit COMSEC material holdings to those operationally necessary to fulfill mission requirements (i.e., normally a single edition). Do not hold full maintenance manuals.

h. Protection of Unattended Facilities:

(1) Secure and guard facilities whenever t hey are left unattended. Because of the many structural variations in these facilities (e.g., vans, aircraft, and open vehicles), standardized criteria for securing them cannot reasonably be prescribed.

(a) Where a facility is inside a solid enclosure (e.g., van or equipment shelter), secure all access points (e.g., windows) from inside, and secure the entrance door with a padlock meeting Federal Specification FF-P-110.

(b) Where this is not practicable (e.g., open vehicle or aircraft), use an approved locking bar or other locking device to prevent tampering or removal of the crypto equipment.

(2) Guard unattended transportable and mobile COMSEC facilities as follows:

(a) Use U.S. guards when the facility contains keying material or keyed crypto equipment.

(b) A roving guard(s) who makes frequent rounds is sufficient protection for facilities located in U.S. or Allied territory.

(c) U.S. guards must be used (and they must be in the immediate area of the facility at all times) for facilities located in non-U.S. or non-Allied territory.

i. Protection of Lock Combinations. Article 515 applies.

j. Firearms. Article 550.e.(3) applies.

k. SOP. Article 550 applies to transportable, but not to mobile COMSEC Facilities.

575. SAFEGUARDING DOD BLACK BULK FACILITIES

a. General. Black bulk facilities operated by or for the DOD use classified crypto equipment to protect multi-channel trunks passing national security-related information. A black bulk facility consists of multi-channel terminal(s) and associated crypto equipment.

b. Definitions:

(1) A Space is the area within a structure occupied by a DOD black bulk facility. A Space may be integrated into an area containing other communications equipment, or it may be a room or enclosure dedicated to the multi-channel terminal(s) and associated crypto equipment only.

(2) A Site is the structure that contains the Space.

(3) Appropriately Cleared means possessing a CONFIDENTIAL or higher security clearance issued by the U.S. Government, or an equivalent clearance issued by a foreign government or an international organization to which the crypto equipment has been released.

c. Safeguarding Criteria. Because of the unique nature of black bulk facilities, they may be operated in many different environments and under varying degrees of security risk. Some requirements are the same as for normal fixed facilities, others are not.

d. General Requirements:

(1) Installation Requirements. Whenever possible, installations should conform to the installation RED/BLACK criteria. The appropriate department or agency authority shall determine the requirement for application of this criteria on a case-by-case basis.

(2) Facility Approvals, Inspections, and Tests. The provisions of Article 550 are applicable. However, TSCM inspections and instrumented TEMPEST tests are not required.

(3) The protection of lock combinations; a determination for the need of firearms; maintaining an SOP; and, the use of nonessential audio/visual equipment are delineated in Article 550.

e. Special Requirements. Annex P contains special requirements for physical security safeguards for DOD black bulk facilities and safeguarding COMSEC material used therein.

CHAPTER 6 - MAINTAINING/MODIFYING A COMSEC MATERIAL ALLOWANCE

CHAPTER 6 - MAINTAINING/MODIFYING A COMSEC MATERIAL ALLOWANCE

601. GENERAL

a. CMIO Norfolk distributes the authorized allowance of (R COMSEC material as validated by the ISIC of the command.

b. COMSEC material in physical form is initially (R distributed via an authorized courier (e.g., Defense Courier Service (DCS)), or issued directly to a Custodian via over -the-counter (OTC) pickup at CMIO Norfolk.

c. Keying material may also be gene rated by selected field sites in electronic form (i.e., 128 -bit key) and distributed physically in a fill device (FD) or transmitted electronically via a telecommunications circuit.

d. The authorized COMSEC material allowance for each command is based on its assigned mission and communications capabilities.

605. COMSEC EQUIPMENT, RELATED DEVICES, EQUIPMENT MANUALS AND OPERATING INSTRUCTIONS ALLOWANCE. An account allowance for COMSEC equipment, related devices, equipment manuals and operating instructions is based upon an approved allowance list in accordance with the following guidelines and/or authorities:

a. Navy, Coast Guard, and MSC Commands :

(1) The type and quantity of cryptographic equipment and related devices that a command is authorized to hold is contained in the NAVY CONSOLIDATED SECURE VOICE AND RECORD/DATA PLAN as validated by CNO.

(2) Shipboard allowances by ship type and/or design are based, in part, upon the guidance contained in OPNAVINST C2300.44 (series).

(3) Additional guidance may also be provided by FLTCINCs, COMNAVSECGRU, COMNAVCOMTELCOM, COGARD TISCOM, Commander, Military Sealift Command), and the Office of Naval Intelligence (ONI).

b. USMC Commands :

(1) As published in individual unit's Table of Equipment (T/E) and/or guidance promulgated by Commandant, Marine Corps//CSB//.

(2) The Commander, Marine Corps Systems Command//C4I2// is authorized to direct transfer of COMSEC equipment and related devices between USMC accounts in conjunction with the fielding of new equipment.

(3) The procedures for modifying allowances of COMSEC equipment and related devices, on a routine and emergency basis that are detailed in Article 655 and 675, respectively, are **not** applicable to USMC commands subordinate to COMMARFOR LANT/PAC, and CGs at the Marine Expeditionary Force (MEF), Division, Aircraft Wing, and Force Service Support Group (FSSG) levels.

(4) CMC, COMMARCORSYSCOM, and the USMC Commanders cited above are authorized to manage the COMSEC equipment and related devices in the CMS accounts of subordinate USMC units.

(a) Temporary transfers, not to exceed eight months, will be accomplished on a local custody basis.

(b) Permanent transfers, in excess of eight months, will be conducted via an SF -153 account -to-account transfer report. Cite this article as authority.

(c) DCMS approval is not required for transfers cited above.

NOTE: CMC//CSB//, COMMARCORSYSCOM//C4I2//, DCMS//30//, and the Chain of Command must be an information addressee on all correspondence directing the permanent transfer of equipment and related devices.

610. VALIDATION OF CRYPTOGRAPHIC EQUIPMENT AND RELATED DEVICES

a. CNO validation and approval is required for all cryptographic equipment and associated ancillary devices that are **NOT** contained in the CNO SECURE VOICE AND RECORD/DATA PLAN (i.e., DON allowance document for cryptographic equipment and related devices).

b. Submit requests for review, validation, and approval using the following format:

ACTION: CNO//N652//

INFO: ISIC
Administrative Chain of Command
CMC//CSB// (USMC commands only)
COGARD TISCOM//OPS4// (CG commands only)
DCMS//30//

Subject: REQUEST FOR CRYPTO EQUIPMENT VALIDATION

(1) Justification for the operational requirement, including the detail that will permit establishment of its relative priority in the general program.

(2) A block diagram of the existing and/or proposed circuit.

(3) The type and general reliability of the transmission medium.

(4) Identification of all terminals on the proposed circuit.

(5) The estimated, average daily volume of classified and unclassified traffic to be handled on the proposed circuit, the maximum classification of that traffic, and any special requirements for such traffic.

(6) Expected use of the proposed circuit.

(7) The nomenclature and quantity of terminal equipment required for the proposed circuit (including an indication of equipment on hand).

(8) Remarks pertinent to compliance with guidance provided by OPNAVINST C5510.93 (series) concerning minimizing compromising emanations or other electromagnetic radiations.

(9) A statement of ability to comply with security criteria, or a description and estimated cost of any modification that may be required.

(10) When landline connections are involved, identify the command that will pay for the telephone lines and/or lease telephone company MODEMs, etc.

(11) A statement that maintenance personnel qualified in accordance with OPNAVINST 2221.3 (series) will be available or that an increase of such personnel will be required to maintain the cryptographic equipment.

(12) Specify the date material needed.

(13) CMS account number.

615. COMSEC KEYING MATERIAL ALLOWANCE

a. The quantity of future editions of keying material (i.e., reserve-on-board (ROB)) to be held by a CMS account is determined by the FLTCINC, CMC, ISIC, or COGARD TISCOM.

b. Factors such as operational requirements, type of command (fixed or mobile), location, duration and area of deployment for mobile units, and the resource limitations and/or geographical constraints of the DCS are to be considered when establishing a standard ROB level for an account. ROB levels can range from 2 to 6 months of keying material (keymat).

620. MAINTAINING RESERVE-ON-BOARD (ROB) LEVEL OF KEYING MATERIAL

a. Each CMS account command must ensure that all effective and ROB editions of authorized holdings are maintained and that requests for increases or reductions are submitted as operational requirements change.

b. It is the responsibility of each CMS account to review their holdings on an annual basis to ensure a continuing need for the quantity and types of all COMSEC material held.

c. Mobile accounts must keep DCS and CMIO informed of their movements (e.g., deployments, underway schedule) to ensure timely delivery of their ROB material.

d. Material that cannot be issued by a CMIO due to insufficient stock levels will be listed below the "Total Lines/Quantity" line on an SF 153 as follows:

FOLLOWING SHORT TITLE(S) ARE YOUR LESS ITEMS:

AKAC 00123 ABC
USKAK 00456 DF

e. As each shipment is received, the Custodian must determine the effective date of each less item. If the ROB level falls **below two months** of keymat, a message must be sent action to DCMS//30//, info the servicing CMIO, indicating the last edition held and requesting assistance in obtaining follow -on editions.

NOTE: Superseded material received in a ROB shipment must be destroyed within 12 hours of opening the shipment. Annotate on the SF 153, "SUPERSEDED UPON RECEIPT." No additional reporting is required.

f. ROB stock level table (**use as a general guide**):

SUPERSESSION PERIODICITY/QUANTITY TO BE HELD (R

ROB LEVEL	Yearly	Semi-annual	Qtrly	Bi-monthly	Monthly	15days	10days	7days
2	1	1	2	2	2	4	6	10
3	1	2	2	3	3	6	9	15
4	1	2	2	3	4	8	12	20
5	1	2	2	4	5	10	15	25
6	1	2	3	4	6	12	18	30
7	2	3	3	4	7	14	21	35

g. ROB quantities are in addition to the effective edition being used. The above table can be used as a **general guide** to (R determine how many editions of keying material are to be held as ROB.
Three months of ROB is standard for most CMS accounts; however, some FLTCINC/TYCOM identified units are authorized to hold 6/7 months of material to support extended operations.

625. MODIFYING RESERVE-ON-BOARD (ROB) LEVEL OF KEYING MATERIAL

a. A request to increase a ROB level requires at least 60 days notice if material is shipped via DCS and at least 30 days notice for material picked up OTC at a CMIO. A request to decrease a ROB level requires a minimum of 14 days notice.

b. Address a request to modify a ROB level as follows:

(1) Navy (see NOTE below), MSC, and USMC supporting establishments :

ACTION: DCMS//30//

INFO: CMC//CSB// (USMC commands only)
Chain of Command
Servicing CMIO

NOTE: USN surface accounts subordinate to a FLTCINC will address their request action to CINCPACFLT or CINCLANTFLT, info ISIC, Chain of Command, DCMS//30//, and servicing CMIO.

(2) Coast Guard Commands :

ACTION: COGARD TISCOM//OPS4//

INFO: Area and/or District Commander
Chain of Command
DCMS//30//
Servicing CMIO

(3) Marine Corps FMF Commands :

ACTION: COMMARFORPAC OR LANT (See NOTE below)

INFO: CMC//CSB//
Chain of Command
DCMS//30//
Servicing CMIO

c. Provide the following information, in sequence, to modify an ROB level:

Subject: ROB LEVEL CHANGE

(1) CMS account number and HCI (e.g., 334455/S).

(2) Current ROB level.

(3) New level.

(4) Effective date in YYMM format.

(5) Servicing DCS and CMIO; indicate any special shipping instructions or whether material will be picked up OTC at the servicing CMIO.

(6) Justification.

NOTE: Marine Corps commands must include message passing instructions to the G -6/CEO, as appropriate (e.g., COMMARFORLANT//G -6//).

d. Action addressees must approve, disapprove or modify a request to change a ROB level for subordinates by sending a message to DCMS//30//, info to the remaining addressees on the original request.

630. DEFENSE COURIER SERVICE (DCS)

a. Defense Courier Service (DCS) is a joint service organization providing courier delivery for qualified categories of classified information to include most COMSEC material.

b. DCS and DCMS are not related service organizations. Each has their own charter and funding responsibilities. DCS budgets annually for its courier service on regular movement missions.

c. Mobile units, exercise planners, and major staff commands requesting allowance changes must allow sufficient time in their notification to DCMS and CMIO to allow maximum use of the regularly scheduled missions.

d. Distribution of COMSEC material is normally accomplished using regularly scheduled DCS missions.

e. Material eligible for shipment via DCS is assigned one of two priorities in the DCS Movement System as follows:

(1) **Regular Movement**: This material, representing the bulk of the material entered into the DCS, moves in accordance with regularly scheduled DCS missions. The majority of COMSEC material is transported via this method.

(2) **Special Movement**: This material is expeditiously moved at the **expense of the requesting command** to satisfy deadlines that cannot be met by regularly scheduled DCS missions. Special movement replaced the former DDD (deadline delivery date) and is normally moved via commercial means based on validated customer needs and available DCS resources.

(a) Commands requesting a special movement must provide a fund site in the request for material and include HQ DEFCOURIERSVC FT GEORGE G MEADE MD//DO// as an ACTION addee. DCMS will coordinate special movements between the requesting command and HQ DCS.

(b) Requests for Special movements will be processed and entered into the DCS system within 48 hours or less.

(c) A request for Special movement **without** a fund site will be transported as a "Regular" shipment regardless of the date the material is required.

635. DEFENSE COURIER SERVICE (DCS) ADDRESS CHANGE

a. CMIOs process and automatically ship ROB material to the DCS delivery address of record for an account (as assigned during the DCS account establishment process) 45 -60 days prior to receipt by an account.

b. To preclude delays in receipt of material, CMS accounts must notify DCMS//30//, and the servicing CMIO and DCS station whenever there is a change in the servicing DCS station or a change in the command address. When there is a change, both the old and new servicing DCS station must be informed of the new address.

640. OVER-THE-COUNTER (OTC) PICKUP FROM A CMIO

a. CMIOs provide over -the-counter (OTC) pickup of COMSEC material for CMS accounts that do not receive their material via the DCS.

b. **ONLY** those commands that will pick up COMSEC material directly from a CMIO are required to have an up -to-date CMS Form 1 on file at the CMIO. The CMS Form 1 lists personnel that are authorized to receipt for and courier COMSEC material between their command and a CMIO. Annex I contains a sample CMS Form 1 and instructions.

c. Pickup of COMSEC material from a CMIO is not authorized unless the CMS Form 1 is up -to-date. There are **NO EXCEPTIONS** to this policy.

d. Personnel picking up COMSEC material must carry proper identification and courier authorization.

e. COMSEC material picked up from a CMIO must be transported directly to the command and be properly stored. Delays or stops, except for emergencies, between the command and the CMIO, are **strictly prohibited**.

645. TERMINATING AUTOMATIC DISTRIBUTION OF COMSEC MATERIAL

a. To terminate automatic distribution via DCS or OTC due to overhaul periods, extended operations outside of normal DCS schedules or delivery locations, etc., advise the servicing DCS station and/or CMIO via message, info DCMS//30//, specifying the inclusive date(s) or months for which keymat is not required.

b. Whenever COMSEC equipment must be removed from an account temporarily or whenever currently held COMSEC keymat will not be used for several months due to overhaul or non -availability, request disposition guidance from DCMS (30). (**NOTE**: USMC commands refer to Article 605.b.)

c. Commands terminating distribution due to disestablishment of a CMS account must follow the procedures in Chapter 8.

d. To resume automatic distribution, notify servicing CMIO via message, info DCMS//30//, a minimum of 60 days prior to the date the material will be needed. Additionally, if applicable, coordinate with servicing DCS station to resume courier service.

650. ROUTINE MODIFICATION OF AN ACCOUNT ALLOWANCE FOR COMSEC KEYING MATERIAL

a. This article is to be used to acquire COMSEC keying material not previously authorized for receipt by the account (i.e., does not reflect in a FLTCINC, TYCOM, or CG area instruction to support deployments). Therefore, Controlling Authority (CA) approval must be obtained prior to acquisition. (A

b. A routine modification to the authorized COMSEC keying material allowance of a command is one which can be met by regular DCS delivery (minimum of 45 days lead-time) or available via OTC service from CMIO (minimum of 7 days lead-time).

c. Requests should be addressed as follows. (**NOTE**: Failure to adhere to the following format could adversely delay keying material acquisition.) (R

(1) USN SURFACE ACCOUNTS SUBORDINATE TO A FLTCINC

ACTION: CINCPACFLT **or** CINCLANTFLT

INFO: Controlling Authority
ISIC
Chain of Command
DCMS//34//
CMIO NORFOLK VA//20//

SUBJ: ROUTINE CHANGE IN COMSEC KEYMAT ALLOWANCE

(2) USN SUBSURFACE ACCOUNTS

ACTION: COMSUBPAC **or** COMSUBLANT

INFO: Controlling Authority
ISIC
Chain of Command
DCMS//34//
CMIO NORFOLK VA//20//

SUBJ: ROUTINE CHANGE IN COMSEC KEYMAT ALLOWANCE

(3) USN SHORE ACCOUNTS

ACTION: Controlling Authority

INFO: ISIC
Chain of Command
DCMS//34//
CMIO NORFOLK VA//20//

SUBJ: ROUTINE CHANGE IN COMSEC KEYMAT ALLOWANCE

(4) COAST GUARD COMMANDS
ACTION: COGARD TISCOM//OPS4//

INFO: Area and/or District Commander
Chain of Command
DCMS//30//
CMIO NORFOLK VA//20//
Controlling Authority

SUBJ: ROUTINE CHANGE IN COMSEC KEYMAT ALLOWANCE

(5) MARINE CORPS COMMANDS
ACTION: Next Senior Flag Level Command (See NOTE below)

INFO: CMC//CSB//
Chain of Command
Controlling Authority
DCMS//30//
CMIO NORFOLK VA//20//

SUBJ: ROUTINE CHANGE IN COMSEC KEYMAT ALLOWANCE

NOTE: Each USMC Flag Level Command (i.e., DIV, Wing, FSSG, MEF) must review and forward their endorsement up the Chain of Command to COMMARFORPAC **or** LANT//G6//, as appropriate. Ensure that message passing instructions to the G-6/CEO are included (e.g., COMMARFORLANT//G-6//).

655. ROUTINE MODIFICATION OF AN ALLOWANCE FOR COMSEC EQUIPMENT, RELATED DEVICES, EQUIPMENT MANUALS AND OPERATING INSTRUCTIONS

a. A request to modify (add/delete a short title or a change in quantity) the authorized allowance of a command for equipment, related devices, equipment manuals and operating instructions must be addressed as follows:

(1) **EQUIPMENT AND RELATED DEVICES**:

(a) **Navy and MSC Commands**:

ACTION: DCMS//30//

INFO: ISIC
Chain of Command
CMIO NORFOLK VA//20// (R

(b) **Coast Guard Commands:**

ACTION: COGARD TISCOM//OPS4//

INFO: Area and/or District Commander
DCMS//30//
CMIO NORFOLK VA//20// (R

(c) **Marine Corps Commands:**

ACTION: Next Senior Flag Level Command (See NOTE below)
INFO: CMC//CSB//
Chain of Command
COMMARCORSYSCOM//C4I2//
DCMS//30//
CMIO Norfolk VA//20// (R

NOTE: 1. CMC Washington DC 021900Z APR 93 delineates USMC procedures for requesting a routine change in COMSEC equipment allowances.

2. Each USMC Flag Level Command (i.e., Div, Wing, FSSG, MEF) must review and forward their endorsement up the Chain of Command to COMMARFORPAC or LANT//G-6//, as appropriate.

3. COMMARFORPAC and LANT endorsements on requests from FMF Commands must be submitted to COMMARCORSYSCOM//C4I2// and requests from Supporting Establishment Commands must be submitted to CMC//CSB//.

(2) **EQUIPMENT MANUALS and OPERATING INSTRUCTIONS:**

ACTION: DCMS//30//
INFO: ISIC
CMC//CSB// (USMC commands only)
COGARD TISCOM//OPS4// (CG commands only)
Area and/or District Commander (CG commands only)
Chain of Command
CMIO Norfolk VA//20// (R

b. Action addressees must approve, disapprove, or modify a request for routine modification from an account by sending a message to DCMS//30//, except for COMMARFORLANT/PAC, info to the remaining addressees on the original request.

c. DCMS//30// must be an addressee on all correspondence involving the permanent transfer of COMSEC equipment, related devices, equipment manuals, and operating instructions.

660. FORMAT FOR ROUTINE MODIFICATION OF AN ACCOUNT ALLOWANCE

a. Multiple short titles may be combined and submitted in a single letter or message. Each short title must be assigned a separate paragraph and the action addressee for each short title must be clearly identified (e.g., 2. FOR DCMS; 3. FOR COMMARFORPAC) in the case of multiple action addressees.

b. Supporting or related items (e.g., manuals for equipment) are not automatically issued when COMSEC material is issued. Each specific item of COMSEC material that is required or associated with a specific item must be requested from the applicable authority. For example, when equipment is ordered for a new installation, the Custodian must also order the required related devices (e.g., fill devices), keymat, maintenance manuals, and operating instructions.

c. The format provided below must be used for routine modification of an account's allowance of authorized holdings of COMSEC keymat, equipment, related devices, maintenance manuals and operating instructions. Where information for a particular short title is not applicable, insert "N/A."

Addees: (as indicated in Articles 650/655)
Subject: (as appropriate)

(1) CMS account number and HCI (e.g., 313131/TS). (R

(2) Short title (indicate mode designator for equipment).

(3) Permanent or temporary (specify dates in YYMM format for temporary (e.g., 9306 - 9310).

(4) Increase or decrease, quantity, and justification (e.g., installation of OTCIXS or TACINTEL, name of exercise).

(5) Present approved allowance (if short title not held, state NONE).

(6) Required ancillary device(s) (e.g., KOI -18, KYK-13).

(7) Date material needed (allow 60 days for delivery via DCS or 7 days if material is to be picked up at CMIO Norfolk). (R

(8) TYCOM and/or ISIC (required only for equipment and related devices).

(9) Validation/authorization (cite CNO authority or equipment master plan for equipment and related devices; no authorization required for one -for-one replacement of defective items).

(10) Servicing DCS station, any special shipping instructions, or indicate OTC pickup from CMIO Norfolk. (R

(11) POC and phone number(s).

665. FORMAT FOR REQUESTING ISSUE OF STANDARD DEPLOYMENT KEYMAT

a. Requests for standard deployment keymat, as listed in the FLTCINC, TYCOM, or CG area instructions, must be submitted a minimum of 60 days before departure from homeport.

b. The following format must be used to request standard deployment keymat and to also indicate partial reductions in the quantity of standard deployment keymat. Where information for a particular item is not applicable, insert "N/A."

ACTION: CMIO (See NOTE below)

INFO: ISIC
DCMS//30//

Subject: DEPLOYMENT ALLOWANCE

(1) CMS account number and HCI (e.g., 323232/S). (R

(2) Ship type (e.g., FF, DDG).

(3) Deployment area (e.g., IO, WP, MED, LANT).

(4) Date material neede d (e.g., 930718).

(5) Inclusive dates material required in YYMM format (e.g., 9307 - 9311).

(6) Cite applicable instruction/authorization.

(7) Any special material required or any special requirements (e.g., partial Reduction(s)).

(8) Servicing DCS station, any special shipping instructions, or indicate OTC pickup from CMIO Norfolk. (R

(9) POC and phone number(s).

NOTE: COMSUBLANT will submit requirements to CMIO Norfolk for deploying submarine accounts.

c. Marine Corps Infantry Battalions involved in the unit deployment program must comply with instructions contained in the "SOP for USMC CMS Account Administration."

670. FORMAT AND ADDRESSEES FOR REQUESTING NEW KEYING MATERIAL

a. The majority of new operational requirements may be satisfied by allocating keymat that is readily available, but not yet designated for a specific purpose. In this situation, the keymat can be provided in a relatively short time (e.g., 2 - 30 days dependent on location and/or delivery options). The opposite case would be a situation which would require that the National Security Agency produce a completely new short title of keymat, requiring a minimum of 120 days notice.

b. The following format must be used to request assignment of a new short title of keymat to support a new or revised operational requirement. Where information for a particular item is not applicable, insert "N/A." Address the request as follows:

(1) Navy (see NOTE below), MSC, and USMC supporting

ACTION: DCMS//30//
INFO: CMC//CSB// (USMC commands only)
Chain of Command
CMIO Norfolk (R

NOTE: USN surface accounts subordinate to a FLTCINC will address their request action to CINCPACFLT or CINCLANTFLT, info ISIC, Chain of Command, DCMS//30//, and CMIO Norfolk. (R

(2) Coast Guard Commands :

ACTION: COGARD TISCOM//OPS4//
INFO: Area and/or District Comman der
Chain of Command
DCMS//30//
CMIO Norfolk (R

(3) Marine Corps FMF Commands :

ACTION: COMMARFORPAC OR LANT
INFO: CMC//CSB//
Chain of Command
DCMS//30//
CMIO Norfolk (R

Subject: REQUEST FOR NEW KEYMAT SHORT TITLE

(1) CMS account number.

(2) Classification of keymat (based on the classification level of information to be protected).

(3) Equipment in which keymat will be used (e.g., KG-84).

(4) Number of copies required.

(5) Use (i.e., operational, maintenance, test).

(6) Inclusive dates in YYMM format (if temporary).

(7) Controlling authority (this will be the command requesting the new keymat).

(8) Date keymat to be effective in YYMM format.

(9) Accounts to hold keymat.

(10) Date material needed (allow a minimum of 120 days for material which must be produced by NSA).

(11) Servicin g DCS station or indicate OTC pickup (only required if originator is to receive the keymat).

(12) POC and phone number(s).

c. Action addressee must approve, disapprove, or modify a request by a command for a new keymat short title by sending a message to DCMS//30//, info to the remaining addressees on the original request.

d. Upon notification from NSA that the request has been approved and a short title assigned, the requesting command must notify DCMS//30// and provide the following information:

(1) Short title (e.g., USKAT 12457).

(2) Classification.

(3) AL code (1, 2, or 4). (R

(4) Controlling authority.

(5) Effective period of key by edition (e.g., edition A effective 1 FEB 94, edition B effective 1 JUL 94).

(6) Long title (i.e., a description of how the material will be used (e.g., KG -84 Operational keytape, KG -84 Operational OTAR KEK)).

675. EMERGENCY MODIFICATION OF AN AUTHORIZED ALLOWANCE

a. An emergency modification of the author ized allowance of a command is one that requires the immediate transfer of COMSEC material to satisfy an urgent and unforeseen operational requirement (as determined by the Commanding Officer).

NOTE: USMC commands must refer to Article 605 for temporary transfers of equipment and related devices.

b. Commanding Officers are authorized to direct the temporary transfer of COMSEC material between CMS accounts to satisfy urgent and unforeseen operational requirements.

c. Temporary trans fer is restricted to no more than two editions of keymat; and a period not to exceed 3 months for equipment or related devices. The temporary transfer is authorized within the following constraints:

(1) The transferring command must not reduce their holdings below the minimum necessary to meet known or reasonably anticipated operational requirements.

(2) The recipient of the material is authorized to hold the material as part of their normal authorized allowance.

d. CRFs, and afloat commands hol ding provisional spare equipment, are authorized to transfer COMSEC equipment and related devices as a replacement for failed equipment submitted in a casualty report (CASREP).

e. After initiating an emergency temporary transfer of (R material, the transferring command must submit a message to the following addressees providing CMS account numbers, short title(s) of COMSEC material transferred, and the rationale for the emergency transfer:

ACTION: Controlling authority (See NOTE below)

INFO: FLTCINC (USN afloat commands only)
CMC//CSB// (USMC commands only)
COGARD TISCOM//OPS4// (CG commands only)

ISICs of transferring and receiving accounts
Recipient of material
DCMS//30//

Subject: EMERGENCY TRANSFER OF COMSEC MATERIAL

NOTE: Do not include DIRNSA as an addressee on emergency transfers of COMSEC equipment and related devices for which they are the CA.

f. Transferring command must cite this article and the request by the originating command (e.g., message, phone call) in the body of the SF 153 as authorization for an emergency transfer of AL 1 and 2 material. (Document the transfer of AL 4 material locally). (R

680. PERMANENT TRANSFER OF AFLOAT COMMANDS TO A NEW OPAREA (R

a. Afloat commands which are permanently re -locating to a homeport in a different ocean area must inform CMIO Norfolk for new OPAREA material 60 days prior to departure from their present homeport.

b. The request will be addressed as follows:

ACTION: CMIO Norfolk

INFO: CINCLANTFLT
CINCPACFLT
TYCOMs and/or ISICs (both areas)
COGARD TISCOM//OPS4// (CG commands only)
DCMS//30//

D)

c. The request must be formatted as detailed in Article 665.b. and include the following additional requirements:

(1) Include stop date, YYMM, for material provided for present OPAREA and start date, YYMM, for material for the new OPAREA.

(2) Request disposition instructions from CMIO Norfolk for that material currently held that is not needed to support the transit to the new OPAREA.

d. CMIO Norfolk is responsible for distributing all material normally held, material required to transit, and the required material to operate in the new OPAREA.

e. Upon arrival at the new homeport, the account must:

(1) Coordinate with applicable DCS commands to effect the change of the servicing DCS station (if not previously done).

(2) Destroy remaining effective segments of keymat from previous OPAREA citing this article as authorization.

CHAPTER 7 - CONTROL AND DOCUMENTATION REQUIREMENTS FOR COMSEC MATERIAL

CHAPTER 7 - CONTROL AND DOCUMENTATION REQUIREMENTS FOR COMSEC MATERIAL

CHAPTER 7 - CONTROL AND DOCUMENTATION REQUIREMENTS FOR COMSEC MATERIAL

CHAPTER 7 - CONTROL AND DOCUMENTATION REQUIREMENTS FOR COMSEC MATERIAL

CHAPTER 7 - CONTROL AND DOCUMEN TATION REQUIREMENTS FOR COMSEC MATERIAL

701. GENERAL

a. The sensitivity of COMSEC material is such that a detailed set of procedures is required to ensure that this material is controlled and properly accounted for at all times.

b. This chapter provides procedures for maintaining the integrity and control of accountable COMSEC material from receipt to disposition (i.e., transfer or destruction).

c. Documentation and reporting requirements for the control of COMSEC material are extensive and require attention to detail. **Accuracy** in the preparation of accounting documents, especially for Electrical Transaction Reports (ETRs) which are rigidly -formatted for computer processing, is an **extremely important** aspect of account management.

d. If, at **any** time you, as a User or Custodian of COMSEC material, are unsure of how to handle a particular requirement or situation, you are strongly encouraged to contact your CMS Custodian, CMS A&A Training Team, or DCMS (as appropriate) for assistance. (**NOTE**: Annex S contains point of contacts for DCMS.)

e. The following outlines the procedures which are addressed in this chapter:

(1) Required CMS account files.

(2) Handling, storage, retention, and classification of CMS account files, records, and logs.

(3) COMSEC material accounting reports (e.g., transfer, destruction, possession, receipt, relief from accountability, inventory, and conversion).

(4) Submitting Receipt and Transfer/Receipt ETRs to DCMS.

(5) Receipting for and conducting pagechecks o f COMSEC material.

(6) Inventorying, issuing, and sealing COMSEC material.

(7) Management of COMSEC material in a watch and Non-watch station environment.

(8) Reproducing and extracting COMSEC material.

(9) Entering amendments.

(10) Destruction procedures for COMSEC material.

703. REQUIRED CMS FILES

Each CMS and LH account will establish and maintain the following CMS -related files:

a. Chronological File.

b. Correspondence and Message File.

c. General Message File.

d. Directives File.

e. Local Custody File.

NOTE: 1. If any of the required files are too large for one file or folder, they may be divided into multiple files.
2. LH files will contain copies of reports, messages, and correspondence, that the account Custodian has determined to be necessary to the effective management of a LH account except for specific requirements listed in this chapter.

706. CMS CHRONOLOGICAL FILE

a. The Chronological File must be used to maintain the following:

(1) COMSEC material accounting reports (e.g., receipt, transfer, destruction, possession).

(2) Running inventory (R/I) (CMS and LH accounts).

(3) Inventory reports (e.g., DCMS-generated SF 153 inventory) and reconciliation notices (**NOTE**: The reconciliation notice is printed at the bottom of the Questionnaire Page of the DCMS -generated SF 153 inventory.) (CMS accounts only).

(4) Transaction log (CMS accounts only).

(5) CMS Form 1 and/or DCS Form 10 (CMS accounts only).

(6) CMS Responsibility Acknowledgement Form.

b. Record copies: Record copies in the Chronological File must be original or exact duplicates of the originals and must include dates and signatures.

c. Working copies: DCMS-generated working copies of inventory reports must be retained until the "Date of Last DCMS-generated SF 153 inventory Reconciled" date is updated on a subsequent DCMS-generated SF-153 inventory provided by DCMS. Retention of the working copy will enable the Custodian to assist DCMS in the resolution of discrepancies, should any occur, during DCMS' inventory review.

709. CMS CORRESPONDENCE, MESSAGE, AND DIRECTIVES FILES

a. The CMS Correspondence and Message File must be used to maintain the following:

(1) CMS account establishment correspondence. (NOTE: Mandatory for accounts established after the effective date of this manual; optional for previously established accounts.)

(2) Custodian and Clerk appointment co rrespondence.

(3) COMSEC incident and PDS reports.

(4) Correspondence relating to command allowance and authorization to store classified COMSEC material.

(5) CMS Updates.

(6) CMS Assist Visit and Inspection correspondence.

D)

b. The CMS GENERAL Message File must contain all effective general messages (e.g., ALCOMs, ALCOMLANT ALFAs) that pertain to account holdings or CMS policy and procedures.

c. The CMS Directives File must contain a copy of each effective directive of the command and higher authority that relates to CMS matters (e.g., guidance for LH accounts/User personnel, Letters of Agreement (LOA), and waivers of CMS policy and procedures).

712. CMS LOCAL CUSTODY FILE. The Local Custody File must contain all effective, signed local custody documents reflecting the issue of COMSEC material.

a. Control of: Custodians and Users must maintain physical control over their local custody documents. This file contains the only documentation of COMSEC material issued locally and access must be controlled appropriately.

b. Completeness of: The Local Custody File must contain a signed document (i.e., SF 153 or locally prepared equivalent form) for each item of COMSEC material charged to the account which has been issued to authorized LHs and Users.

715. HANDLING, STORAGE, RETENTION, AND CLASSIFICATION OF CMS FILES, RECORDS, AND LOGS

a. Handling and storage : CMS files, records, and logs must be handled and stored in accordance with their overall classification. These items are not COMSEC material.

b. Retention periods : Annex T contains the minimum retention periods for CMS files, records, and logs.

c. Inactive records : When placed in an inactive status, CMS files, records, and logs must be clearly labeled with the appropriate classification and the authorized date of destruction. When practical, all material to be destroyed during the same general timeframe should be grouped together, (e.g., material authorized for destruction based on a retention period of two years from 1992, may be destroyed in January 1995).

d. Classification guidance :

(1) The following will be classified a minimum of CONFIDENTIAL:

(a) Reports that list two -person -control (TPC) material.

(b) Reports which contain a complete record of classified keying material held by an account.

(c) Reports which indicate the effective date of classified keying material.

(2) The following additional general guidance is provided:

(a) Although individu al reports (e.g., transfer and destruction) are "For Official Use Only" (FOUO), a file holding a classified report must be classified accordingly. Likewise, a file containing classified inventory reports must also be stamped with its applicable classification.

(b) Any report or file containing classified information will be classified according to the highest classification of the information contained therein.

(c) Each report or file which contains classified COMSEC or COMSEC -related informa tion will also bear, in addition to the classification, the following statement:

"Derived from: CMS 1 (R
Declassify on: XI" (R

(d) Classification is the responsibility of the Custodian and must be determined by evaluating the content of each report or file. If in doubt, consult OPNAVINST 5510.1 (series) or contact DCMS//20// for guidance.

718. USE OF FORMS AND COMPUTER DISKS

a. Locally prepared forms may be created at the discretion of an account. All locally prepared forms must contain the same information, including signature data, as the sample forms shown in this manual.

b. Computer -generated forms may also be used at the discretion of an account. Spreadsheet, database, or other software packages may be used provided they contain all of the information required by this manual (or that appear on official, preprinted forms such as SF 153s).

(1) Commands that maintain computer -generated records should keep an up -to-date printout of all records in the CMS Chronological File at all times.

(2) **ANCRS Users** will maintain copies of their R/I and Transaction Number (TN) Log in accordance with the following:

TYPE OF COMMAND	FREQUENCY OF PRINTOUTS	RETENTION PERIOD
Submarine	Prior to putting to sea.	Destroy when replaced with updated versions.
Surface or Deployed Mobile Units	Once a month.	Destroy when replaced with updated versions.
Shore or Non -Deployed Mobile Units	Once every 3 months.	Destroy when replaced with updated versions.

(3) The requirements for signatures, where required, may not be waived. Computer -generated records must allow for signatures on printouts.

(4) Computer -generated forms that would normally have material lined out must either allow for a separate area for lined out items or have an extra column to indicate that the item has been lined out. Items that would normally be lined out must not be deleted until the retention times in Annex T have been met.

c. Computer disks : Disks (both floppy and hard) can become corrupted by a variety of things such as spikes, static, power surges, magnets, etc. To protect against the potential loss of critical accounting data, CMS Custodians who maintain automated accounting files will adhere to these minimum requirements:

(1) Non-mobile commands must use one floppy diskette to back up accounting files.

(2) Mobile commands (including ships) must use two floppy diskettes to back up accounting files.

(**NOTE**: It is highly recommended that all commands use two diskettes for back up purposes and that the diskettes be alternated to prevent the loss of data or disk failure that can occur due to frequent use of a single diskette.)

d. Back-up requirement : Back up your accounting files at the end of each computer session that modifies your R/I and Transaction Number (TN) Log.

721. CMS LIBRARY. All CMS accounts must maintain a CMS Library which consists of the following manuals and instructions: (R

a. Automated Navy COMSEC Reporting System (ANCRS) Users Guide.

b. CINCLANTFLT/CINCPACFLT/CINCUSNAVEURINST C2282.1 (series) - Basic Shipboard Allowance of COMSEC Material. (USN surface CMS accounts only).

c. CMS 1 (series) - CMS Policy and Procedures Manual.

d. CMS 3 (series) - CMS Inspection Manual.

e. CMS 5 (series) - CMS Cryptographic Equipment Information and Guidance Manual.

f. CMS 6 (series) - STU-III Policy and Procedures Manual.

g. COMDTINST M5500.21 - Coast Guard Information Security Program Manual. (COGARD accounts only)

h. COMSUBLANTNOTE 2280 (series) - Basic COMSEC material allowance for Submarine Force (Submarines only).

i. EKMS 702.01 - STU-III Key Management Plan.

j. NAG 16 (series) - Field Generation and Over-the-air Distribution of Tactical Electronic Key. (Required only if account involved in OTAT/OTAR operations).

k. NSA Mandatory Modification Verification Guide (MMVG).

l. OPNAVINST 2221.5 - Release of COMSEC Material to U.S. Industrial Firms Under Contract to USN. (required only by those accounts who have occasion to release COMSEC material to contractors).

m. OPNAVINST 5040.7 - Naval Command Inspection Program.

n. OPNAVINST 5510.1 - Information and Personnel Security Program Regulation.

o. OPNAVINST 5530.14 - Physical Security and L oss Prevention.

p. Procedures Manual for Over -the -Air Key Transfer (OTAT) and Over -the -Air -Rekeying (OTAR). (Required only if account involved in OTAT/OTAR operations).

q. SPCCINST 2300.4 - Utilization and Disposal of Excess COMSEC Material.

r. SPCCINST 5511.24 - Classified Electronic COMSEC Material in the Navy Supply System.

s. OPNAVINST 2221.3 - (Qualifications of Maintenance Personnel) (Article 610 refers.)

(A

NOTE: CMS account Custodians must ensure that their LH commands have access to or are provided copies of all CMS manuals and instructions required in the operation of the LH account.

724. CMS TRANSACTION LOG

a. The CMS Transaction Log is used to record and assign a sequential transaction number (TN) to accounting reports which are reportable to the DCMS COR.

b. Annex U contains a sample CMS Transaction log and procedures for maintaining this log. This log may be reproduced for use by Custodian personnel.

NOTE: A copy of the TN log must be attached to all Fixed -Cycle and Combined Inventory reports submitted to DCMS//30//.

727. COMSEC MATERIAL ACCOUNTING REPORTS

a. COMSEC Material Accounting Reports (e.g., SF -153s) provide an audit trail for each item of accountable COMSEC material. These reports may be prepared manually or be computer -generated.

b. Specific requirements for submitting reports to DCMS and retention of documentation at the local level are provided in the articles below that address each particular type of report.

c. The various reports and a brief description of their general use is as follows:

(1) Transfer Report : Used to document and/or report the transfer of COMSEC material from one CMS account to another CMS account or one holder to another holder (i.e., local custody issue).

(2) Destruction Report : Used to document and/or report the physical destruction of COMSEC material.

(3) Possession Report : Used to document and report possession of COMSEC material.

(4) Receipt Report : Used to document and/or report receipt of COMSEC material. (NOTE: Usually combined with a transfer report.)

(5) Relief from Accountability Report : Used to document and report the loss of AL 1 or AL 2 COMSEC material.

(6) Conversion Report : Used to document and report the removal of old short titles and/or accounting data from the DCMS COR data base and the entry of new data. (NOTE: Submitted only when directed by DCMS.)

(7) Inventory Report : Used to document and report the physical inventory of COMSEC material.

d. Selected reports must be submitted electrically while others require submission of the actual paper accounting report. Regardless of the reporting method used, timely and accurate submission of accounting reports will ensure that the DCMS COR data base properly reflects all COMSEC material charged to a CMS account.

e. Annex V addresses signature requirements and procedures for completing SF 153 COMSEC Material Accounting Reports.

730. GUIDANCE FOR SUBMITTING REPORTS TO DCMS

a. Reports which are eligible for submission to the DCMS COR via an Electrical Transaction Report (ETR) must be forwarded as indicated herein (in priority order):

(1) Via the COMSEC Automated Reporting System (CARS) using a PC and a STU -III **OR**

(2) Via the General Service (GENSER) AUTODIN Communications Network in message form.

NOTE: Do **not** forward SF 153s to DCMS for reports that have been submitted electrically via CARS or message.

b. ONLY selected "Receipt" and "Transfer/Receipt" reports will be submitted via an ETR. Article 742 contains specific guidance for submitting ETRs. Also, Annex F and W contain procedures for formatting/submitting ETRs via CARS or in message format, respectively.

c. As a **last** resort, when **no** other method is available, accounts can submit paper accounting reports to the DCMS COR via first class mail for unclassified, first class mail for CONFIDENTIAL within the U.S. (includes possessions and territories), or registered mail for CONFIDENTIAL outside of the U.S.

733. TRANSFER REPORT

a. **Defined**: A transfer is the physical movement of COMSEC material between two CMS accounts. There are two types of transfers:

(1) Account -to -Account (Intra -DON) Transfer : The transfer of COMSEC material between two DON CMS accounts.

(2) Inter -Service Transfer : The transfer of COMSEC material between a DON CMS account and the CMS account of another service (e.g., Army or Air Force), agency (e.g., NSA, DACAN, SECAN), department (e.g., State Department), nation, or commercial contractor.

NOTE: The following statement must be placed in the body of inter -service SF 153 Transfer Reports originated by DON CMS accounts:

"The above material will be removed from DON COR files and be brought on charge to the above service/agency account number effective 90 days after the transfer date above. Return the original SF-153, properly signed and dated to: (**NOTE:** transferring command will insert its address here)."

b. Transfer Authorization:

(1) Keying Material and Manuals. The transfer of COMSEC keying material marked or designated CRYPTO, and AL 1 and AL 2 COMSEC manuals must be authorized in accordance with the applicable transfer authorization indicated in this manual, DCMS, or the controlling authority (CA) of the material.

(a) CAs are listed in the CMSR or on the material itself (e.g., Letter of Promulgation for manuals).

(b) Any transfer which constitutes a temporary or permanent modification to the authorized holdings of an account must be handled in accordance with Chapter 6.

(2) Equipment and Related Devices. The transfer of COMSEC equipment and related devices must be authorized in accordance with Chapter 6.

D)

c. Documentation Requirements:

(1) An SF 153 Transfer Report must be prepared and forwarded with all shipments.

(2) Transferring accounts will prepare an original and two copies of an SF 153 Transfer Report for all inter-service shipments. The original and one copy will be forwarded with the shipment. One copy will be retained in the transferring command's files pending receipt of the original. (R

(3) Transferring accounts will prepare an original and one copy (two copies when transferring AL 4 to CMIO Norfolk or a cache account) of a SF 153 Transfer Report for all intra-service shipments. The original will be forwarded with the shipment and the copy will be retained in the transferring command's files pending acknowledgement of receipt by the recipient. (R

(4) The transfer of AL 4 COMSEC material between DON CMS accounts (except CMIO Norfolk and the cache account) or users will use the local custody issue procedures detailed in Article 769. (R

d. Reporting Requirements:

(1) The transfer of AL 1 or AL 2 COMSEC material between DON CMS accounts must be reported to DCMS via a Transfer/Receipt (RETR"S" or a Receipt ETR"R" prepared by the recipient of the material (**NOTE**: See Article 742 for receipt procedures.)

736. DESTRUCTION REPORT

a. General:

(1) Destruction of COMSEC material requires the presence of two appropriately cleared and authorized persons.

(2) The destruction report must be completed immediately after the material is destroyed. Destruction will be completed within the timeframes contained in Article 540.

(3) Normally, destruction of COMSEC material will be documented on an SF 153 and retained locally. Destruction reports will be submitted to DCMS **ONLY** when directed to do so by DCMS.

(4) Document destruction of individual segments (i.e., tape segments, days, pages, etc.) of COMSEC material using the forms and guidance contained in Figure 7-1, 7-2, or 7-3, as appropriate. Destruction of entire editions will be documented on the SF 153 using the guidance contained in Annex V, as appropriate.

b. Documentation and Reporting Requirements.

(1) COR Reportable Destruction Requirements. Destruction will be reported to DCMS by mailing the SF 153 Destruction Report **ONLY** when directed to do so by DCMS. (**NOTE**: Destruction reporting to DCMS will be restricted to accounts being disestablished and other special occasions as determined by DCMS (e.g., when local destruction of obsolete AL 1 or AL 2 equipment is authorized by DCMS).

(2) Local Destruction Documents:

(a) The destruction of COMSEC material will be documented and retained locally using a SF 153, or locally prepared equivalent form (e.g., CMS 25). Annex V contains guidance for preparing the SF 153 local destruction document.

(b) Local destruction records must be completed to docopR ed i

(c) Local destruction records are mandatory for all AL 1 and AL 2 COMSEC material, regardless of classification.

(d) Local destruction records are optional for AL 4 COMSEC material classified CONFIDENTIAL and below, (R regardless of CRYPTO markings.

NOTE: Copies of required destruction reports used by LHs/Users (e.g., CMS 25 or equivalent), when the original is forwarded to the CMS Account Custodian, will be retained or disposed of IAW local command directives.

739. POSSESSION REPORT. An SF 153 Possession Report is used to return AL 1 or AL 2 COMSEC material to proper accountability controls **or** to report the reproduction of AL 1 or AL 2 COMSEC material. A Possession Report must be submitted for a whole edition, complete short title, or separately accountable end item of AL 1 or AL 2 COMSEC material on the following occasions:

a. When AL 1 or AL 2 COMSEC material is reproduced. (**NOTE**: See Article 781 for guidance on reproducing COMSEC material.)

b. When AL 1 or AL 2 material comes into the possession of a CMS account by other than a properly documented transfer or receipt (e.g., no SF 153 and originator unknown).

c. When AL 1 or AL 2 material previously charged to the account is found and documentation exists to show that the material was transferred or lost, and lined out on the running inventory.

NOTE: Each of the above situations (except authorized reproduction) requires submission of a COMSEC Material Incident Report in accordance with Chapter 9 before submitting a Possession Report to DCMS.

d. Do **not** submit an SF 153 Possession Report whenever a whole edition, complete short title, or separately accountable AL 1 or AL 2 material is found that was documented as destroyed, but follow these instructions:

(1) Report the finding of the material as a PHYSICAL incident in accordance with Article 945.

(2) If the material is authorized for destruction, destroy it and document the actual destruction locally. Indicate in the report of the incident that the found material was destroyed.

(3) If the found material is not authorized for destruction (e.g. found material is equipment or future key that was previously reported as "prematurely" destroyed), request disposition instructions in the incident report.

e. Do not submit a Possession Report for AL 1 or AL 2 COMSEC material that is properly documented as charged to the account but is found outside of proper storage. This situation will, require submission of a COMSEC Material Incident Report in accordance with Chapter 9.

742. RECEIPT REPORT

a. Reporting Criteria:

(1) Material received from DCMS, CMIO or Cache Account: (R

(a) All AL 1, 2, or 4 material received from DCMS (078000), CMIO Norfolk (078002), or NAVCOMTELSTA Sicily (360109) (R must be reported to DCMS (and the originator of the shipment) using a Receipt ETR transmitted via CARS or message.

NOTE: NCTS Sicily is the only CMS Cache account in the DON.

(b) When a Receipt ETR message is used to receipt for material from the above accounts, do not return the SF 153 to the originator. Complete the SF 153 and file it in the CMS Chronological File with a feedback copy of the Receipt ETR message attached to it.

(c) When a Receipt ETR is submitted via CARS, the SF 153 must be completed and returned **only** to NCTS Sicily.

NOTE: Do **not** forward copies of corresponding SF 153s to DCMS or CMIO for Receipt ETRs submitted via CARS or message.

(2) Material received from a DIRNSA account:

(a) All AL 1, 2, or 4 material received from DIRNSA will be reported to DCMS using a Receipt ETR transmitted (R via CARS or message **and** DIRNSA.

(b) When a receipt ETR message is used to receipt for material from DIRNSA, do not return the SF 153 to DIRNSA. Complete the SF 153 and file it in the CMS Chronological File with a copy of the Receipt ETR message attached to it.

(c) When a Receipt ETR is submitted via CARS, the SF 153 must be completed and returned to DIRNSA.

(d) The DIRNSA assigned delivery control number, transaction number, date, and the names of both recipients must be listed in the "REMARKS" section of a Receipt ETR for TPC material received from DIRNSA.

(e) Transaction numbers used by DIRNSA consist of only five digits. Therefore, when using ETR Receipt procedures, the last digit of the CY must precede the 5-digit TN assigned by DIRNSA. For example, DIRNSA TN 05678 in CY 93 would be shown as "305678."

(3) Material received from a DON CMS account :

(a) AL 1 or AL 2 material received from a DON CMS account other than DCMS (078000), CMIO, or NAVCOMTELSTA Sicily, (R must be receipted for by submitted Transfer/Receipt ETRs to DCMS which **must** be prepared by the **recipient** of the material.

(b) If a Transfer/Receipt ETR message is used to receipt for material from a DON CMS account, do not return the SF 153 to the originator. Complete and sign the SF 153 and file it in the CMS Chronological File with a feedback copy of the Transfer/Receipt ETR message attached to it.

(c) When a Transfer/Receipt ETR is submitted to DCMS via CARS, the SF 153 must be completed and returned to originator.

NOTE: Do **not** forward copies of corresponding SF 153s to DCMS for Transfer/Receipt ETRs submitted via CARS **or** message.

(4) Material received from all other accounts:

AL 1, 2, or AL 4 material received from all other CMS accounts (e.g., Army, Air Force, contractors) must be reported to DCMS and the originator via an SF 153 only.

b. Timeframe for Reporting Receipt:

(1) A receipt must be forwarded within 96 hours after receiving COMSEC material.

(2) The 96 hour clock begins either from the time the material is picked up from a command (e.g., CMIO) **or** from the time the material is received at the command (e.g., DCS courier).

(3) If emission control (EMCON) or MINIMIZE is in effect (which precludes a message from being forwarded), report receipt via CARS or mail.

c. Discrepancies:

(1) Report inner package damage, evidence of tampering, or incorrect shipping methods in accordance with Chapter 9.

(2) Report contents discrepancies (i.e., material in the shipment does not correspond with the material listed on the SF 153) to shipment originator via message.

(3) Report discrepancies in the material itself (e.g., pagecheck errors) in accordance with Annex X.

745. RELIEF FROM ACCOUNTABILITY REPORT

a. A Relief from Accountability Report is submitted to DCMS whenever a whole edition, complete short title, or separately accountable end item of AL 1 or AL 2 material is missing and no documentation exists which indicates that the item was either transferred or destroyed.

b. The CMS account charged with the material must submit a COMSEC Material Incident Report in accordance with Chapter 9 in addition to the SF 153 Relief from Accountability Report.

748. CONVERSION REPORT

a. An SF 153 Conversion Report is used to remove old short titles and/or accounting data from the DCMS COR data base and replace them with new data.

b. This report is actually two separate reports, one will delete a short title/accounting data from account records and one to add the correct data into account records.

c. Conversion reports are submitted only when specifically directed by DCMS.

751. RECEIVING AND OPENING COMSEC MATERIAL SHIPMENTS

a. General: COMSEC material is shipped to your account by your servicing CMIO, via the DCS, or it may be picked up OTC from your servicing CMIO.

b. DCS Form 10: To receipt for material from the DCS, your account must present an up-to-date DCS Form 10 to the DCS courier(s).

c. CMS Form 1: To pick up material from a CMIO, you must have an up-to-date CMS Form 1 on file at the CMIO.

d. Summary of processing steps upon opening COMSEC material:

(1) Inspect the inner wrapper for signs of tampering.
(2) Open the shipment.
(3) Inventory the contents.
(4) Conduct Protective Packaging inspection.
(5) Conduct pagechecks as required by Annex Y.
(6) Apply status information (less equipment).
(7) Add COMSEC material to running inventory R/I).
(8) Receipt for the material.
(9) Complete transaction log.
(10) Properly store the material.

e. Who May Open COMSEC Material Shipments:

(1) All COMSEC **keying material** shipments must be opened by **two** persons, one of whom must be the Custodian (or Alternate). The other person may be any properly cleared and authorized witness. The presence of two persons is necessary in the event that TPI is required for keying material.

(2) Two people are not required to open other COMSEC shipments, however, two people are strongly recommended for ease of verifying the contents against the enclosed SF 153.

NOTE: Personnel other than Custodians are authorized to assist Custodians (or Alternates) in opening and processing material shipments, providing they are properly cleared and are under the d irect supervision of a Custodian (or Alternate).

(3) Opening of a Shipment by other Than the Intended Account :

(a) If a COMSEC material shipment belonging to another account is inadvertently opened by a Custodian or Alternate, the contents of the shipment must be inventoried immediately.

(b) The package must be resealed immediately and promptly forwarded to the proper command. The body of the enclosed SF 153 must be annotated as follows:

"**NOTE: Package number (____) was opened inadvertently (date) by (name of command), account number (_____). The contents were inventoried (date) and the shipment sealed immediately.**

Signed: (signature of Custodian or Alternate of command that inadvertently opened the package).

Witnessed: (signature of witness)."

(c) If the SF 153 Transfer Report in the package that was opened inadvertently is incorrect or missing, use the procedures in the following paragraphs to correct or prepare an SF 153. If an SF 153 must be prepared, ensure the above note is placed in the body of the SF 153.

NOTE: All personnel who regularly receive and process mail and packages addressed to the command (e.g., mailroom or administrative personnel) must be advised **not** to open packages specifically marked for the account or Custodian.

754. REQUIRED ACTIONS UPON RECEIPT OF COMSEC MATERIAL

a. **STEP I**: Inspect packages for tampering : Upon receipt of a COMSEC material shipment, immediately inspect the inner shipping wrapper for damage or evidence of tampering. If evidence of either is found, retain the wrappings and submit a COMSEC Incident Report in accordance with Chapter 9.

b. **STEP II**: Inventory the Contents : Inventory the contents of the shipment against the enclosed SF 153 Transfer Report and comply with the applicable instruction below:

(1) Shipment contents do not correspond exactly to SF 153 Material Listings: Follow the instructions in Step III.

(2) No SF 153 enclosed, but originator known: Follow the instructions in Step IV.

(3) No SF 153 enclosed and originator **NOT** known: Follow the instructions in Step V.

(4) SF 153 enclosed, contents correspond exactly: Follow the instructions in Step VI.

c. STEP III: Contents Discrepancy:

(1) Correct the SF 153 listing to reflect exactly the material in the package, and initial all corrections (Custodian (or Alternate) and a properly cleared and authorized individual).

(2) Report the nature of the discrepancies to the originator of the shipment via message.

(3) Then follow the instructions in Step VI to report the receipt.

d. STEP IV: No SF 153 enclosed, originator known:

(1) Forward a message to the originator listing the short titles and accounting data of the contents and request confirmation of the shipment contents. Also request an outgoing TN and date to complete the Transfer Report.

NOTE: If a message cannot be used, forward a facsimile or letter to DCMS/ /30// listing the short titles and accounting data of the contents.

(2) Retain all packaging material and shipping containers until the discrepancy is resolved.

(3) Enter the material on the R/I.

(4) After verification of the contents of the shipment and receipt of an outgoing TN from the originator, prepare an SF 153 and report receipt of the shipment in accordance with Article 742.

(5) If verification from the originator of the shipment is not received within 7 days, follow the procedures in Step V.

e. STEP V: No SF 153 enclosed, originator **NOT** known:

(1) Forward a message, facsimile, or letter to DCMS//30// stating the circumstances and listing the short titles and accounting data of the contents.

(2) Retain all packaging material and shipping containers until the discrepancy is resolved.

(3) Submit an SF 153 Possession Report in accordance with Article 739 and Annex V.

f. STEP VI: Complete SF 153 Transfer Report and Report Receipt: Complete the SF 153 Transfer Report and submit a receipt in accordance with Article 742.

757. CONDUCTING PAGECHECKS AND VERIFYING COMPLETENESS OF COMSEC MATERIAL

a. Pagechecks are conducted to ensure the completeness of COMSEC material (except for protectively packaged material) and COMSEC related material.

b. COMSEC equipment, related devices, and components must be verified for completeness well in advance of their installation/use so that there is ample time to obtain replacement equipment or parts, if required.

c. The Custodian must establish internal procedures to ensure that all COMSEC material received by an account is pagechecked and/or verified for completeness in accordance with this manual.

d. Certification of completed pagechecks for COMSEC publications and keying material must be recorded on the Record of Pagechecks (ROPs) Page for the material, or on the front cover for material having no ROPs Page.

e. Pagecheck Requirements: Minimum pagecheck requirements for all COMSEC material are contained in Annex Y. Some requirements are repeated here for emphasis and because of the unique procedures that must be followed.

(1) Do not open sealed crates containing COMSEC equipment or sealed/resealed packages of keying material for the sole purpose of complying with the pagecheck upon receipt requirement.

(2) Pagecheck unsealed COMSEC keying material upon initial receipt, upon transfer, during all account inventories, during daily watch -to-watch inventory, and prior to destruction.

(3) Unsealed AKAI (daily changing call signs) and AKAV (Communication Electronic Operating Instructions (CEOI)) are exempt from the requirement to pagecheck each copy upon initial receipt. Recipients need only check one or two copies of each new edition upon receipt to ensure page and print continuity.

(4) Inspect protectively packaged keying material upon receipt in accordance with the applicable Protective Technologies Pamphlet.

f. Procedures: Each item of printed COMSEC material contains a list of effective pages (LOEP), either on a separate page or on the front cover of the material. This list indicates which pages should be in the publication and identifies the status of each page (i.e., an original page or a specific amendment number page). (NOTE: CMS 5 (series) contains listings of components that comprise a complete COMSEC end -item equipment.)

(1) To conduct a pagecheck of printed COMSEC material, compare each page in the publication being checked against its LOEP.

(2) Each page listed on the LOEP must be in the publication and each page must reflect the correct status. For example, pages identified on the LOEP as "ORIGINAL", must be ORIGINAL pages. Pages identified on the LOEP as being a specific amendment page (e.g., 1 or AMEND 1), must be that specific amendment page.

g. **Requirement to Verify Mandatory Modifications**: Verify the installation of DON and NSA mandatory equipment modifications in accordance with Annex Y using CMS 5 (series) and/or the NSA Mandatory Modification Verification Guide (MMVG) as follows:

(1) The Custodian will inspect the MOD Record Plate on all COMSEC equipment and have a qualified maintenance technician internally verify the installation of mandatory modifications **prior to an account-to-account transfer**. Use CMS 5 (series) to determine DON mandatory and optional modifications and the MMVG to determine NSA mandatory modifications.

(2) Should an examination of the equipment indicate a requirement to install a mandatory modification, the Custodian will ensure that the mandatory modification is installed by an appropriately qualified maintenance technician as specified in the instructions accompanying the modification.

(3) Before transferring equipment, the Custodian will also ensure that the modification or MOD Record Plate on COMSEC equipment accurately reflects all installed modifications.

NOTE: See Annex Y (Pagecheck Chart) for additional pagechecking requirements for other COMSEC material.

h. Reporting Pagecheck or Other Discrepancies: If a discrepancy is noted during the pagecheck and verification procedures of COMSEC material, the discrepancy must be reported in accordance with Annex X.

760. APPLYING STATUS INFORMATION TO COMSEC MATERIAL

a. Status information (i.e., effective and supersession date) must be annotated on all COMSEC keying material and COMSEC accountable manuals and publications upon receipt **except** for large accounts (i.e., 500 or more line items). Large accounts must enter status information on the ANCRS running inventory and annotate the status information upon issue to local holders or users.

b. Status information for keying material can be located in the CMSR (DON keymat) and AMSG -600 (keymat designated for NATO use), and is also promulgated via message (e.g., ALCOMLANT ALFA, JOINT STAFF ICP MANAGER MACDILL AFB, FL).

c. The status of COMSEC manuals and publications is normally listed on the Letter of Promulgation (LOP) page within these documents. When not listed, the originator of the document promulgates status via separate correspondence.

NOTE: Since the status of COMSEC material may be affected by loss, compromise, or operational deviations, CMS Custodians must determine the most current status of material prior to issue, transfer, and destruction.

d. Procedures for Applying Status Information:

(1) Canister-packaged keying material:

Status will be applied to canister -packaged keying material using either a grease pencil, non -permanent ink or marker (i.e., ink markings that can be completely and easily removed for canister inspection), or a zip -lock bag as detailed below:

(a) Grease pencil or non -permanent ink or marker: Only grease pencils or non -permanent ink or marker may be used to apply status directly to the outside of a canister. The use of permanent ink markers/pens for this purpose is **prohibited** as these markers inhibit proper canister inspection.

(b) Ziplock bag: Apply an adhesive label to the outside of the ziplock bag with the short title of the keymat, edition and the effective and supersession dates annotated on the label. Enclose the associated keying material canister in the ziplock bag.

NOTE: When using the ziplock bag, the adhesive label can be color-coded to help distinguish between 1 -month and 2-month key. For example, a white label could be used to identify 1 -month key, a yellow label (using a yellow highlighter to "paint" a white label) to identi fy 2-month key.

NOTE: Applying tape or other labels directly to the surface of keying material canisters is strictly **prohibited**. This unauthorized practice can only serve to hide intrusion or penetration efforts and hamper inspection procedures.

(2) **Other Protectively Packaged Keying Material:**

(a) The status of other protectively packaged keying material sealed in its original packaging must be marked on the plastic wrapper.

(b) Upon opening the keying material for use, transfer the status information to the front cover of the material.

(3) COMSEC Material in Book or Booklet Form, Manuals, and Publications: Apply applicable status information on the outside front cover so that it does not cover any manufacturer printed data.

763. CMS RUNNING INVENTORY (R/I)

a. The CMS Running Inventory (R/I) must be maintained by all CMS and LH accounts and is used to record **all** AL 1 through AL 4 COMSEC material held by an account.

b. Annex Z contains procedures for maintaining (i.e., required information, additions, deletions, etc.) the R/I.

c. R/Is may be manually prepared or computer-generated. In either case, an up-to-date copy which reflects material held by the account should be maintained in the Chronological File at all times.

d. **ANCRS users** will maintain their R/I in accordance with the documentation provided with the ANCRS program and Article 718.

766. CMS INVENTORIES

a. COMSEC material must be inventoried as follows:

(1) **Semiannually:** COMSEC keying material assigned AL 1 through AL 4 must be inventoried semiannually (twice each calendar year (CY)).

(a) The results of one of the two semi-annual inventories of AL1 and AL2 material must be reported to DCMS, once a year, in accordance with Article 766.b.(1).

(b) The results of the two semi-annual inventories of AL 4 keying material will be retained at the command in accordance with Annex T.

(2) **Annually:** AL 1, AL 2, and AL 4 COMSEC equipment and publications/manuals must be inventoried annually.

(a) The results of the AL 1 and AL 2 equipment and publications/manuals must be reported to DCMS//30//, once a year, in accordance with article 766.b.(1).

(b) Inventory results of AL 4 equipment and publications/manuals must be retained at the command in accordance with Annex T.

(3) **Change of Command:** All COMSEC material will be inventoried and the inventory results retained at the command in accordance with Annex T. (**NOTE:** An inventory upon change of a SCMSRO is not required, but is at the discretion of the Commander).

(4) **Change of Custodian:** All COMSEC material will be inventoried and the results will be retained at the command in accordance with Annex T.

(5) **Disestablishment:** An inventory must be conducted as part of the disestablishment process. Chapter 8 contains the specific requirements for disestablishing a CMS account (CA).

b. There are three types of CMS inventories (i.e., FIXED-CYCLE (FC), SPECIAL, and COMBINED). The following pertains:

(1) **FIXED-CYCLE (FC) SF 153 Inventory** :

(a) The purpose of the FC Inventory is to ensure that all accounts satisfy the national requirement for a semiannual inventory of keymat and an annual inventory of equipment and publications.

(b) Twice each CY, at six-month intervals, and as determined by your COMSEC account number (see FC Inventory Schedule), DCMS will generate and place on the Front End Processor (FEP), or mail to your account, a FC inventory.

(c) The inventory and procedural check-off sheet generated for your account during the first half of the calendar year (CY) (January through June) **must be completed and returned to DCMS no later than 60 days** after the preparation date of the FC Inventory. (This date appears in block 3 of the inventory.) This FC inventory must be completed in its entirety (i.e., all key, equipment, manuals/publications must be inventoried.)

(d) The FC inventory generated for your account during the first half of the CY (January through June) is the **only** inventory DCMS will reconcile for that CY.

(e) The FC inventory you receive during the second half of the CY (July through December) need not be completed in its entirety. Only your key holdings must be inventoried. Do not report the results of this inventory to DCMS, but document the results and retain locally in accordance with Annex T.

(f) The following table will help you determine when your account can expect to receive its FC inventories.

FIXED-CYCLE (FC) INVENTORY SCHEDULE

If your CA number is :	**1st** FC Inventory for CY :	**2nd** FC Inventory for CY :
100000 through 158500	January	July
158501 through 199999	February	August
200000 through 258100	March	September
258101 through 299999	April	October
300000 through 358200	May	November
358201 through 399999	June	December

EXAMPLE: If your CA is 123456, DCMS will generate your first FC inventory in January of each CY. This is the FC inventory that must be completed in its entirety (i.e., key, equipment, and publications must be inventoried) and returned to DCMS for reconciliation. In July of each CY, your account will receive its second FC inventory. Only the key portion of this second inventory must be completed. The results of this second inventory will be retained locally.

(g) To identify your FC Inventory on the FEP, look for files preceded by your CA and an ".inv" and ".chk" suffix (e.g., 123456.inv, 123456.chk).

(h) If you receive a FC Inventory, either on the FEP or via mail, out of synch with the above schedule, destroy it locally in accordance with OPNAVINST 5510 (series). Do not report this destruction to DCMS.

(i) Non-receipt of your FC SF 153 Inventory does not relieve you of your responsibility to comply with the minimum inventory requirements of this article. Contact DCMS, Operations Department (30), if you cannot download and/or locate these files on the FEP during your scheduled FC inventory months.

D)

(2) SPECIAL SF 153 Inventory :

(a) The purpose of the SPECIAL inventory is to satisfy the Navy requirement to conduct and document Change of Command and Custodian inventories.

(b) This DCMS-generated SPECIAL SF 153 inventory is available at command request for the purpose of conducting and documenting the mandatory Change of Command and Change of Custodian Inventory.

(c) A DCMS-generated SPECIAL SF 153 Inventory is also available at command request to document a Change of SCMSRO, Alternate Custodian, or Local Holder Custodian. A SPECIAL inventory, for these purposes, is not required by Navy CMS policy but is at the discretion of the CO.

D) (d) The results are retained at the command in accordance with Annex T and are not reported to DCMS. (R

(3) COMBINED SF 153 INVENTORY :

(a) This inventory may sometimes be used to satisfy both the requirements for a FC and a SPECIAL inventory.

(b) A FC inventory may be COMBINED with a SPECIAL inventory when, and only when, the occasion for the SPECIAL inventory will not interfere with the command being able to return the completed inventory to DCMS no later than 60 days after the preparation date of the FC inventory report.

(c) When combining an SF 153 FC inventory with a SPECIAL inventory, the COMBINED inventory **must** be completed in accordance with this article and Annex AA.

c. Miscellaneous CMS Inventory Policy :

(1) Extended Absence of Custodian . If the CMS Custodian is or will be absent for more than 60 days, a new CMS Custodian **must** be appointed and a Change of Custodian Inventory conducted.

(2) Waiver of Inventory Requirements in a COMBAT Environment :

(a) When operations in a combat environment preclude completion of a required CMS inventory, the requirement is automatically waived until operational circumstances permit inventory completion.

(b) Commands so affected must destroy their DCMS-generated SF 153 FC inventory and notify DCMS//30// by message as soon as practicable that submission of the required FC inventory will be delayed. When circumstances permit resumption of normal account activities, DCMS must again be notified by message.

(c) Upon receipt of your notification that normal account activities have resumed, DCMS will generate a SF 153 FC inventory for your account.

(3) Inventory of Material in Spaces to which the CMS Custodian is **NOT** normally Authorized Access :

(a) Regardless of its intended use, CMS Custodians and Alternates who receive, issue, account for, store, and control COMSEC keying material that is used to protect Sensitive

Compartmented Information (SCI)/Special Intelligence (SI), do not require SCI/SI indoctrination unless they also require access to SCI/SI.

(b) Keymat designated for SCI/SI circuits is not in and of itself SCI/SI. Custodians and/or Alternates who are not SCI/SI-indoctrinated must not be refused access to SCI spaces when such access is required to conduct an inventory or periodic reviews of the local CMS accounting procedures. The command will make advance arrangements to sanitize spaces long enough to allow the Custodian to complete account business.

(c) If operational considerations preclude allowing either the Custodian or Alternate access to a space, the individual responsible for the COMSEC material in the spaces must provide the Custodian with a properly completed local inventory, and must certify in writing that all required pagechecks were conducted, and inform the custodian of any pagecheck discrepancies.

(4) Inventory of Material Issued on Local Custody :

(a) A Custodian may direct LHs or Users to inventory the COMSEC materials for which they have local custody responsibility.

(b) When so directed, the LHs or Users will visually verify the short title, edition, and accounting number of the COMSEC materials they have signed for on local custody. The account Custodian is encouraged, however, to conduct the sight inventory of material held on local custody when possible, particularly on the occasion of a SPECIAL inventory.

(c) Results of a LH or User inventory must be reported in writing to the Custodian. The inventory may be recorded and reported on an SF 153 or another form previously approved by the Custodian.

(d) Local inventories will be retained at the command in accordance with Annex T, and not be forwarded to DCMS.

(5) Material Temporarily held by a CRYPTO Repair Facility (CRF) or Maintenance Pool :

(a) Material temporarily (i.e., less than a year) in the custody of a CRF or a maintenance pool may be inventoried by sighting the local custody document for the material.

(b) If the material has been in the custody of the CRF or maintenance pool for more than 1 year , the CRF or maintenance pool must verify, in writing to the Custodian, that the equipment is in their custody, or the Custodian must personally sight the equipment.

d. **Requesting a DCMS-Generated SF 153 Inventory :**

(1) CMS accounts will automatically receive their FC SF 153 inventories in accordance with Article 766.b.(1).

(2) If a FC inventory is not received, notify DCMS//30// by message.

(3) The Custodian must request a SPECIAL inventory from DCMS, as follows: (R

(a) Request for SPECIAL inventory must be submitted via message to DCMS//30//.

(b) The subject line must read: " **REQUEST FOR SPECIAL INVENTORY**," and provide the following:

1 Command title.

2 Account number.

3 Reason for inventory (i.e., **mandatory** for Change of Command and Custodian; optional for Change of SCMSRO, Alternate Custodian, LH and Alternate LH Custodian).

4 Date DCMS should place inventory on CARS FEP for downloading by accounts, or date DCMS should mail inventory (as applicable). If a CARS user, date should be five working days before DCMS inventory is actually required. If inventory is being mailed, date should be 30 days before the DCMS inventory will actually be required.

5 Mailing address only if inventory to be mailed to account.

NOTE: CMS accounts must keep DCMS, DCS, and CMIO Norfolk advised of any change in their command title and/or permanent mailing address including zip code). (R

e. **Documenting a CMS Inventory :**

(1) A FC or a COMBINED inventory must be documented on a DCMS-generated SF 153.

(2) The result of an inventory which is not to be returned to DCMS for processing (i.e., SPECIAL, LH, and local inventories of AL 4 material) may be documented using a DCMS-generated SPECIAL Inventory, SF 153, as appropriate. (R

(3) A DCMS-generated inventory will not list AL 4 materials "charged" to an account (see article 766.f.). Accordingly, accounts with AL 4 material holdings will need to locally generate a SF 153 inventory that lists these locally accountable materials. The custodian and witness will then use both documents (i.e., the DCMS-generated SF 153 inventory and the locally-prepared SF 153 (listing AL 4 material holdings)) to complete and document the inventory. (R

f. **Format of a DCMS-Generated SF 153 Inventory :**

(1) Each DCMS-generated inventory will consist of the following sections:

(a) Inventory Procedural Check-Off List.

(b) SF 153 Inventory report (alphanumeric listing of material charged to account).

(2) The inventory lists all AL 1 and AL 2 keying material charged to the account as well as all in-transit (IT) or in-transit and pending destruction (IT PD) AL 1, AL 2, and AL 4 keying material as of the report preparation date. (R

(3) The inventory also lists all AL 1 and AL 2 equipment and publications/manuals charged to the account as of the report preparation date as well as all AL 1, AL 2, or AL 4 equipment and publications/manuals IT or IT and PD AL 1, AL 2, or AL 4 publications/manuals.

g. **Conducting an Inventory :**

(1) Who May Inventory COMSEC Material :

(a) A COMBINED or SPECIAL Inventory conducted due to a Change of Custodian must be conducted by the outgoing Custodian and witnessed by the incoming Custodian.

(b) If the outgoing Custodian is physically incapacitated, the inventory must be conducted by the incoming Custodian and the Primary Alternate Custodian of the account.

(c) All other inventories must be conducted by the account Custodian (or Alternate) and a qualified witness.

(d) LH Inventories must be conducted by the LH Custodian (or Alternate) and a qualified witness.

(e) User Inventories must be conducted by the User having local custody responsibility for the material and a qualified witness.

(2) How to Inventory COMSEC Material :

(a) All individuals conducting an inventory must sight the short title, edition suffix, and (if applicable) accounting (serial/register) number of each item of AL 1, AL 2, AL 3, or AL 4 COMSEC material held by the command.

(b) Unsealed COMSEC materials and the classified components of issued repair or Q -kits must be pagechecked during an inventory.

(c) Annex Y details pagecheck requirements.

769. ISSUING COMSEC MATERIAL

a. Responsibility :

(1) Custodians are responsible for all COMSEC material held by their account and must control COMSEC material in accordance with this manual.

(2) Movement of all COMSEC material within a CMS account must be coordinated with the CMS Custodian.

(3) Movement of COMSEC material between LH accounts, between LHs and Users of different CMS accounts, or between different command CMS accounts, must be conducted as authorized by the Custodian.

(4) COMSEC material will be issued for use only after determining that the intended recipient is properly cleared and authorized to hold/use COMSEC material.

NOTE: COMSEC material designated as SCI/SI can be issued to SCI/SI cleared personnel only.

(5) All personnel receiving COMSEC material must be provided written instructions for properly safeguarding, handling, and accounting for COMSEC material.

NOTE: Non -DON personnel (e.g., Army, Air Force) are only required to adhere to national doctrine which mandates TPI handling/storage for TOP SECRET key only.)

(6) The issue of COMSEC material must be documented in order to maintain an audit trail for accountability purposes in the event the status of the material changes (e.g., supersession, compromise).

b. Local Custody Defined :

(1) Local custody is the acceptance of responsibility for the proper handling, safeguarding, accounting, and disposition of COMSEC material issued by Custodians and User personnel.

(2) Every person to whom COMSEC material is issued must complete a CMS Responsibility Acknowledge Form in accordance with Annex K.

c. Local Custody Issue Forms :

(1) An SF 153, CMS 17 card, or a locally prepared equivalent form may be used to properly document the local custody issue of COMSEC material. The minimum information required on locally prepared forms is as follows:

(a) A statement of responsibility.
(b) Issued by.
(c) Issued to.
(d) Short title, quantity, accounting (serial/register) number and AL code(s) of material issued.
(e) Date.
(f) Signature(s).

(2) The issuing Custodian must retain the original copy of the signed and dated local custody document and provide a copy to the individual receipting for the material. A signed local custody form indicates assumption of responsibility for the material listed thereon.

d. CMS Local Custody File :

All CMS and LH Custodians must maintain a local custody file containing effective, signed local custody documents.

e. Time Periods for Issuing COMSEC Material :

(1) Equipment, publications, and other material not marked or designated CRYPTO may be issued at any time prior to the effective date of the material.

(2) COMSEC keying material in hard copy form marked or designated CRYPTO, may not be issued any earlier than 30 days prior to the effective period (month) of the material.

NOTE: Authorization to issue keying material marked or designated CRYPTO more than 30 days before its effective period must be obtained from DCMS//20//.

(3) LHs and Users may be issued a one edition of WHENDI (when directed) material.

f. Issue of COMSEC Keying Material In Hard Copy Form to Mobile Users:

Mobile users (i.e., Marine Tactical units, Naval Special Warfare (SPECWAR) units, Naval Construction Battalion units, Mobile Inshore Undersea Warfare units, and Explosive Ordnance Disposal (EOD) units, and all aircraft) are authorized issue of a sufficient quantity of keying material to support mission requirements. (**NOTE**: Mobile users in this instance does not include U.S. ships). Issue keying material as follows:

(1) Paper Copy Form Under **Normal** (Peacetime) Conditions :

(a) When possible, issue paper copy key as whole editions in order to preserve the integrity of the protective packaging.

(b) If it is necessary to issue extracts or segments of paper copy key, no more than three segments (effective plus two) of any short title will be issued. The segments will not be removed from the protective packaging until immediately before issue.

(c) If more than three segments of a short title are required to complete a mission, the entire edition will be issued.

(d) During issue, the issuing Custodians and Users will verify and acknowledge receipt of the segments and then jointly reseal the non -effective segment(s) as outlined in Article 772.

(e) Airborne units that are issued the entire edition and require frequent access to the final copy of a multicopy keytape segment during rotating flight operations, are authorized to place the final keytape segment in a ziplock bag with the original canister of material (i.e., the loose segment need not be sealed in an envelope). Mission essential material will be issued as close to the start of the mission as possible.

(2) Paper Copy Form Issue Under **Combat** Conditions :

(a) In combat operations, key must be issued in electronic form whenever possible, either in the equipment or in a FD.

(b) During combat operations, the issue of an entire canister or edition of key to front -line positions must be avoided (when key is not issued in electronic form).

NOTE: See Annex AD for the maximum amount of keying material that may be issued in a DTD under realworld crisis/ contingency scenarios/combat conditions. (A

(c) In combat operations, up to seven segments of keying material (effective plus six) may be issued to individuals who must be separated from their command or the CMS issuing point for more than one cryptoperiod (when key is not issued in electronic form).

(3) Keying Material in Electronic Form:

(a) If keying material is issued to a user via a FD, loading of the FD and issue to the user will occur just prior to the planned mission.

(b) Issue/receipt of the loaded FD will be in accordance with the TPI requirements for FDs outlined in Chapter 5.

NOTE: 1. Issuing custodians are authorized to prematurely extract paper key from its protective packaging for the purpose of downloading the key, in electronic form, into a FD. (A

2. When electronic key converted from keytape is loaded into a FD, the keytape segments can be destroyed unless there is an operational requirement to retain them until superseded. If retained until superseded, they must be stored and accounted for in accordance with article 775e(2). (A

(c) Electronic key in a FD which is superseded during a mission will be zeroized within 12 hours of supersession. (**NOTE:** Exceptions to the 12-hour destruction standard are outlined in Chapter 5 and Annex A to the "Procedures Manual for Over-the-Air-Transfer (OTAT) and Over-the-Air-Rekey (OTAR)."

(d) Upon mission completion, remaining effective key stored in a FD will be zeroized by User personnel before returning the FD to the Custodian. The Custodian must ensure that a FD is zeroized immediately upon its return.

g. Issue and Receipt of Electronic Key in a FD:

(1) Recipients of electronic key transferred in a FD must acknowledge receipt of this key by signing local custody documents.

(2) Minimum accounting information for the key must include the short title or designator, date of generation and/or loading, number of copies made, date of transfer, identity of issuers and recipient, classification, CA, and effective period of the key, and the serial number of the FD.

(3) Each location holding electronic key in a FD must properly safeguard and continuously account for the loaded FD by serial number, until the key is zeroized, overwritten, or otherwise destroyed.

h. Local Custody Issue Limitations :

(1) Issues to a CRF or Other Repair Facility :

(a) COMSEC equipment and related devices issued to a Crypto Repair Facility (CRF), a tender, or a maintenance pool element for repair and return must be issued using local custody procedures.

NOTE: When using local custody procedures, the material remains on charge to the "transferring" CMS account and must be inventoried during account inventories.

(b) When COMSEC equipment will be repaired by a CRF and local custody procedures will be used, prior to pick-ups/drop-offs, Custodians must submit a message directly to the CRF. The message must identify command personnel authorized to courier COMSEC equipment to and from the CRF.

(c) Due to the paperwork involved, account -to- account transfer procedures should only be used when it is known that the equipment will be at the repair facility for an extended period of time, or, the equipment has to be shipped to the repair facility because it is located a considerable distance from the account command.

(2) Manuals Required to Study for Advancement :

CMS accounts are authorized to issue accountable COMSEC or COMSEC -related manuals on local custody to personnel of subordinate or nearby active -duty units in preparation for advancement examinations or for use in taking CMS/COMSEC correspondence courses. Ensure that personnel are properly cleared and have facilities, if required, for storing classified COMSEC or COMSEC -related manuals.

(3) Issue to Deployed Local Holders or Users of Another CMS Account :

(a) When account holdings permit, Custodians are authorized to issue material on local custody, on request, to deployed LH Custodians or Users of another CMS account provided:

(1) The deployed LH Custodian or User requesting the material is authorized to hold the material.

(2) The transferring command does not reduce their holdings below the minimum necessary to meet known or reasonably anticipated requirements.

(b) Reproduced copies or extracts should be used whenever possible. (**NOTE**: See Articles 781 and 784 for procedures on reproducing and extracting COMSEC material, respectively.)

(4) CMS Account Support to Remote Local Holders :

(a) Occasionally, a LH command or unit will be remote from its parent CMS Account and will also be unable to obtain necessary material as a LH from a CMS account in the local area.

(b) Under the above circumstances, direct issue from a CMIO to the LH is permitted (after determining that the intended recipient is appropriately cleared and authorized to hold the requested material). In this situation, the LH may hold up to three months ROB (i.e., effective plus three months of future material). (NOTE: The procedures in this paragraph do not apply to mobile users.)

(5) Issue of COMSEC Material by a Training or School Command :

At a training or school command, local custody issue must be used to provide accountable COMSEC training and study material to authorized personnel in a training status.

772. SEALING COMSEC MATERIAL

a. Unsealed COMSEC material, at the Custodian or User level, after its initial pagecheck, will be sealed or resealed in accordance with the guidance contained in this article.

b. The account Custodian will specify in local command instructions who (i.e., Custodian or User) has responsibility for sealing or resealing COMSEC material.

c. Unsealed COMSEC material is sealed or resealed under the following conditions:

(1) To avoid daily pagechecks and destruction of superseded segments (e.g., if part of an issued effective edition of, extractable keying material (except keying material packaged in canisters) that will not be used for a significant period of time (e.g., two or more days)).

(2) When all segments in a canister are intentionally removed due to a packaging or production defect.

(3) When the last segment of keying material packaged in a canister (i.e., last segment of single copy keytape (segment 31 or 62) and the final copy of multiple copy segments (3/03)) is extracted for use and its effective period exceeds 24 hours.

(4) When a segment(s) of keying material is unintentionally removed from its protective packaging before its effective period.

d. The unintentional removal of key from its protective packaging before its effective period must be recorded on the destruction record of the material.

(1) Removal of key is defined as key pulled loose from a keycard book or, in the case of canister -packaged key, segments pulled out of the canister and not detached or segments detached from the canister.

(2) The documentation of unintentional removal must include:

(a) A statement that the material was unintentionally removed.
(b) Date of removal.
(c) Identity of segment(s) actually removed.
(d) Signature(s) of the individual(s) who removed the key.

(3) Key discovered removed from its protective packaging (as described above) before its effective period with no documentation certifying that the removal was unintentional, must be reported as a COMSEC incident in accordance with Chapter 9.

e. Intact or an entire edition of multiple copies of the **same** short title and **same** edition may be sealed in the same envelope; however, each serial/register number must be listed on the outside of the envelope when using the alternative sealing procedure in para h. (2) of this article.

f. Sealing loose or segmented keying material of the same days key from multiple copies or short titles in the same container or envelope is **prohibited.**

g. Only future segments of key may be sealed. All segments superseded prior to the date the material will be sealed, must be destroyed and recorded on the destruction document of the material.

NOTE: Do not place a partially completed destruction record for segmented material inside a sealed envelope. Annotate its location on the outside of the envelope and store it with the material in a zip -lock bag or other container.

h. Sealing procedures:

(1) Unsealed segmented material may be considered resealed when placed in a container (e.g., zip -lock bag or a binder with plastic document protector pages) which will reasonably prevent the segments from being lost or misused.

(2) **IF** the following **alternative** method is used, adhere to the following guidance:

Use an opaque (i.e., non -transparent) envelope, record the following information on the outside of the envelope:

(a) Short title.
(b) Edition.
(c) Accounting (serial/register number(s)).
(d) AL code.
(e) Classification.
(f) Status.
(g) If material to be sealed is segmented, identify the specific segments (e.g., days 7 -31, segments 10 -62).

NOTE: Pagecheck segmented material prior to placing it an envelope.

i. When material sealed in its original production wrapper or resealed in accordance with this Article is opened, the material must be pagechecked and all superseded segments must

be removed and destroyed immediately, and the destruction recorded on the destruction record of the material.

j. Keying material packaged in canisters is considered to be protectively packaged and sealed in its original canister.

775. COMSEC MATERIAL MANAGEMENT IN A WATCH STATION ENVIRONMENT

a. **Watch Station Defined:** An area which is occupied and operates on a 24-hour, 7-day a week basis; an 8-hour, 5-day a week basis; or any similar basis (e.g., Combat Information Center (CIC), ships bridge,) is defined as a watch station.

b. **Custody:** All COMSEC material held or used at a watch station must be signed for on a local custody document.

c. **Responsibility:** While on duty, each watch supervisor is responsible for all COMSEC material listed on the watch-to-watch inventory, regardless of which watch supervisor signed the local custody document for the material.

d. **Inventory Requirements:**

(1) A watch station must maintain a watch-to-watch inventory which lists all COMSEC material held (including accountability of resealed segments/material).

(2) The material will be listed by short title, edition, accounting number, and quantity.

(3) All paper keying material will be inventoried by sighting its short title, edition and accounting number. Equipment may be inventoried by quantity only.

NOTE: If an equipment requiring key is operating properly, the keycard/segment may be verified as present in the equipment on that basis.

(4) The inventory must be designed to provide a means of recording dates and initials or signatures to certify that the inventory was conducted.

(5) An inventory of all COMSEC material held by a watch station must be conducted whenever watch personnel change.

(6) The inventory will be conducted by appropriately cleared and authorized personnel as designated by the oncoming watch supervisor. (**NOTE:** In the case of COMSEC material requiring TPI, the inventory must be signed by the two individuals who completed the inventory.)

e. **Pagecheck Requirements:** All unsealed keying material (except keying material packaged in canisters), publications, and equipment held by the watch station must be pagechecked/verified in accordance with Article 757 and Annex Y. Unsealed keying material includes:

(1) Keytape segment(s) that may have been uninten-tionally removed from its canister before its effective period and not yet resealed in accordance with Article 772.

NOTE: Ensure that resealed COMSEC material is accounted for during watch -to-watch inventories.

(2) Keytape segment(s) that cannot be destroyed immediately after use because there is an operational requirement to retain the key until it is superseded. The still -effective segment must remain under TPI, be resealed, properly stored, and accounted for until it is superseded and destroyed.

(3) Superseded extract(s) or segment(s) of keying material which is awaiting destruction, including extracts or segments which have been placed in a special access control container (SACC) securely welded to the interior of a GSA -approved security container.

(4) The last copy of a multiple -copy key segment which was removed from its canister and is being held until superseded. If the material will not be destroyed within 24 hours, the material must be resealed in accordance with Article 772 and added to the watch -to-watch inventory.

(5) Key in loose leaf manuals or booklet form (e.g., AKAC 874).

f. **Discrepancies:** Any inventory discrepancies must be reported immediately to the Custodian or Alternate Custodian. If the discrepancy is determined to be a COMSEC incident, it must be reported in accordance with Chapter 9.

g. **Status Information:** The effective and supersession date for all COMSEC material (less equipment, related components and devices) held by the watch station must be clearly marked on the material in accordance with Article 760.

h. **Destruction:**

(1) Destruction of superseded material must be accurately documented and conducted within the required timeframe.

(2) Article 790 contains destruction procedures. Chapter 5 delineates personnel, methods, and time periods for destroying COMSEC material.

778. COMSEC MATERIAL MANAGEMENT IN OTHER THAN A WATCH STATION ENVIRONMENT

a. **General:** Areas where COMSEC material is required to perform a communications function and the area is not a watch station (e.g., mobile users, CRF, and Intermediate Maintenance Facility work-bench areas) will manage COMSEC material in accordance with this article.

NOTE: Mobile users are defined as Marine Tactical units, Naval Special Warfare (SPECWAR) units, Naval Construction Battalion units, Mobile Inshore Undersea Warfare units (MIUWUs), Electronic Ordnance Disposal (EOD) units, and all aircraft.

b. **Custody:** All COMSEC material must be issued using a local custody document.

c. **Inventory Requirements**: A watch-to-watch inventory listing of COMSEC material is not required. The local custody issue document will serve as the record of inventory. Document completion of inventories on the front or reverse side of the local custody document. An inventory will be conducted in accordance with the following guidance:

(1) Aircraft:

(a) Upon change of crew personnel.
(b) Upon issue of material to aircrew personnel.
(c) Upon turn-in of material to a Custodian.
(d) COMSEC material will be handled as follows when end of mission results in a stop prior to returning to home airfield:

(1) At a U.S. Military controlled airfield: Keying material will be stored at a near-by secure facility or will be securely stored onboard the aircraft in a security container that is mounted in or internally chained to the aircraft structure. If the material is stored at a location other than the aircraft, place a listing of the contents inside of a protective container with the material (e.g., inside a double-locked metal box, a double-locked briefcase or a double-wrapped box). Generate a hand receipt for the sealed container. On the receipt, annotate the highest classification of material placed in the container. Do not give any outward indication on the container of its contents. Obtain proper signatures on the hand receipt and provide the individual(s) storing the container with a copy of the receipt.

(2) At a civilian or non-U.S. Military controlled airfield and a near-by secure storage facility will not be used or is unavailable: Securely store the material onboard the aircraft (as noted above) and check the aircraft and storage container every 24 hours for signs of tampering.

NOTE: If the storage container(s) on the aircraft protecting keying material is damaged or indicates evidence of possible tampering, conduct an inventory immediately. In the event of a discrepancy, submit a COMSEC incident report, as soon as possible, in accordance with Chapter 9.

(2) Mobile Users (less aircraft):

(a) Conduct an inventory of COMSEC material prior to departure and upon return to garrison (or the location where the Custodian issued the material).

(b) An inventory is not required while conducting exercises or actual operations remote from your garrison (or the location where COMSEC material is issued).

(3) CRF and Intermediate Maintenance Facility Work -bench Areas:

COMSEC material held in these areas will be inven-toried in accordance with Article 766 (i.e., inventory COMSEC equipment and publications annually and keying material semiannually).

(4) LHs/Users (when access to COMSEC material is not required on a daily basis; e.g., material accessed once a week for key/rekey purposes):

(a) Material need not be inventoried daily provided:

(1) TPI access and handling rules are strictly enforced.

(2) Custodian is confident that proper control can be maintained for material without a daily inventory and accompanying written record.

(b) LHs/Users need not open security containers for the sole purpose of conducting an inventory. However, if the security container is opened for any reason and LHs/Users have access to the material, an inventory will be conducted at that time along with the destruction of superseded material.

d. Pagecheck Requirements: Pagecheck COMSEC material in accordance with Article 757 and/or any local instructions provided by the issuing Custodian.

e. Destruction: Conduct destruction in accordance with this manual or, in the case of mobile users, the instructions provided by the issuing Custodian.

781. REPRODUCING COMSEC PUBLICATIONS AND KEYING MATERIAL (R

a. Definition: Reproduction of COMSEC material is the complete reproduction of an **entire** code, authenticator, call sign (CAC), publication, or keylist (regardless of the reproduction method). Reproduction of less than an entire copy of material is an extract. Extracts are prepared in accordance with Article 784.

NOTE: Reproducible material is defined as material printed on paper which can be duplicated by writing, typing, or xeroxing. Reproducible material does not include material coded by an arrangement of holes (e.g., segmented tapes).

b. Authority to Reproduce: To satisfy an operational requirement, the CO may authorize the reproduction of an entire edition of CAC material authorized to be held by the account. This authorization takes precedence over any restrictions or prohibitions against reproducing copies which may be contained in the Handling Instructions (HI) or Letter of Promulgation (LOP) of the material. In addition, further reporting to higher authority of the fact of reproduction is not required.

c. Restrictions on Reproducing a CAC. The following CAC material may **not** be reproduced:

(1) Any U.S., Allied, or NATO Nuclear Command and Control Material.

(2) AKAA 285, AMSA TC 2, AMSA TX 9000, AMSA 661, AMSA 622, and AMSC E/D 640.

d. Preparation of Reproduced Copies:

(1) Only an original copy is authorized for use in reproducing COMSEC material.

(2) Copies may not be reproduced from a reproduced copy.

e. Control of Reproduced Copies. The CO of the command with local custody responsibility for the reproduced COMSEC material is responsible for controlling reproduced copies.

D)

f. Accountability of Reproduced Copies: (R

(1) AL 1 and AL 2 reproduced copies of COMSEC material must be reported to DCMS//30// by submitting a SF 153 Possession Report in accordance with Article 739 and Annex V.

(2) AL 4 reproduced copies of COMSEC material are not accountable to DCMS. AL 4 reproduced material is accounted for and handled based on its assigned classification.

NOTE: Reproduced AL 4 COMSEC material received from CMIO Norfolk, cache, or non-DON account must be reported to DCMS using an SF 153 (see Article 742).

(3) Subsequent accounting for the reproduced copies is the same as that of the original material.

g. Classification of Reproduced Copies. Reproduced copies of COMSEC material must be assigned the same classification and special markings (e.g., CRYPTO, NOFORN) as the original material.

h. Handling of Reproduced Copies:

(1) Copies of reproduced material must be handled the same as the original material, according to classification, special markings (if any), and AL code.

(2) Classified reproduced copies may not be transmitted on-line, and may not be disassembled for wider distribution.

(3) Unclassified reproduced copies may be disassembled for wider distribution only within the command.

i. Restrictions on CAC Reproduction. The Commanding Officer can authorize local reproduction for local command use. (A This assumes original is held by command (i.e., command is validated to hold CAC by CA). When reproduced for local use, account for locally; handle in accordance with classification of original CAC; do not enter into CMCS. The following applies:

(1) **Non-emergency situation**: CAC can be reproduced for transfer to another command only after obtaining CA permission, information copy to DCMS//30//. Reproduced CAC, if AL 1 or AL 2 must be entered into CMCS.

(2) **Emergency situation**: The CO can authorize reproduction of CAC for transfer outside of command; with after-the-fact reporting to CA and DCMS//30//. Reproduced CAC must be entered into the CMCS.

j. Procedures to Enter CAC into CMCS: (A

(1) Command that reproduced the CAC must submit SF 153 Possession Report to DCMS; and,

(2) Transfer reproduced material on SF 153 to requesting command.

k. Assignment of Short Titles and Accounting Data . Short titles and accounting data will be assigned to reproduced copies by the preparing CMS account Custodian or Alternate in accordance with the following procedures:

(1) The same short title (including any edition suffix), classification, and AL code of the original material must be assigned to each reproduced copy.

(2) Assignment of accounting numbers to AL 1 reproduced copies, together with the four digit suffix, as described in NOTE below, will be used to assign an accounting number to reproduced copies.

NOTE: If the accounting numbers contains more than four digits, use only the last four digits of the original accounting number. A four digit suffix beginning with 001 will then be appended to each reproduced copy along with the original accounting number in a one-up sequence as described below.

EXAMPLE: 1. If 30 copies are to be reproduced from USKAK 9999 EE accounting number 123456, the short title and accounting number of the first reproduced copy would be "USKAK 9999 EE 3456001." The second reproduced copy would be "USKAK 9999 EE 3456002," and so on.

2. **ANCRS** Users must enter the prefix letters that precede the accounting number (in parenthesis) in the short title field (e.g., USKAK 9999 (AB)).

l. Listing Reproduced Copies on Accounting Documents :

(1) Each individual reproduced copy of AL 1 material must be listed on a separate line of an account document.

(2) Since reproduced AL 2 and AL 4 material will not have an accounting number, this material will be listed as a single line entry with the total quantity listed in the quantity column/field of the accounting document.

m. Local Custody Requirements for Reproduced Copies . Local custodian requirements for reproduced copies are the same as for original copies.

n. Transfer of Reproduced Copies :

(1) Transfer Authorization . Transfer of reproduced copies of COMSEC material requires authorization from the Controlling Authority. (R

(2) Transfer Report :

(a) An SF 153 Transfer Report must be prepared if reproduced COMSEC material is transferred to another command. Cite the authority for the transfer in the body of the SF 153 Transfer Report.

(b) Article 733 details procedures for transferring COMSEC material.

784. PREPARING EXTRACTS FROM COMSEC PUBLICATIONS AND KEYING MATERIAL

a. Definition:

(1) An extract is defined as a portion or segment of a COMSEC publication or keying material.

(2) An extracted portion or segment is physically separate from the material from which it is prepared, either as a result of physical removal, manual reproduction (i.e., writing, typing, or xeroxing).

(3) References to, or statements revealing the gist or main point of a paragraph, an article, or a section of a publication are not extracts, nor are brief quotations used in correspondence or messages.

(4) Extracts may be issued on a local custody document to another CMS account only when they are authorized to hold the material or for use within the command extracting the material.

b. Authority to Prepare Extracts :

(1) Emergency situation : To satisfy an emergent operational requirement, the CO may authorize the preparation of extracts from any COMSEC material authorized to be held by the account.

NOTE: This authorization is applicable to both unclassified and classified material and takes precedence over any restrictions or prohibitions against extracting material

(2) **Classified** Extracts in a Non -emergency situation :

During non -emergency situations, the following sources constitute authorization for preparing classified extracts:

(a) LOP, HI, forward page, or text of the publication.

(b) Separately promulgated directive affecting a series of publications.

(c) Controlling authority of the material when the above sources do not address extraction.

(3) **Unclassified** Extracts in a Non -emergency situation :

During a non -emergency situation, this article, i n the absence of specific directives to the contrary, constitutes authorization to prepare extracts of unclassified material regardless of the overall classification of the publication.

(4) Special Authorization for Training and School Commands :

(a) Service schools and training commands are authorized to make extracts of classified information from any COMSEC material authorized to be held by the command for training purposes only .

(b) Extracts may not be removed from the school or training command, and shall be accounted for and destroyed locally.

c. Controlling Classified Extracts :

The CO of the command with local custody responsibility for the extracts is responsible for controlling classified COMSEC extracts.

d. Classification of Extracts :

Extracts from classified COMSEC material will be classified and assigned any applicable special markings (e.g., CRYPTO, NOFORN) in accordance with the following procedures:

(1) If individual paragraphs or other subdivisions of a classified publication are not assigned a classification and special markings, and if no classification guidance is included in the publication itself, the extract shall be assigned the same classification and special marking as that of the overall publication.

(2) If individual paragraphs or other subdivisions of a classified publication are assigned a classification and special markings, the extracts shall be assigned the classification and special markings as the paragraph or section from which the extracts are made.

e. Disassembling COMSEC Publications :

(1) To permit wider dissemination only within a command, the CO may authorize the Custodian or LH Custodian, to make a temporary subdivision of an unclassified COMSEC publication.

(2) Classified COMSEC publications may not be disassembled for dissemination within or outside the command.

f. Local Custody Requirements :

(1) Extracts of COMSEC keying material marked CRYPTO will be documented on local custody forms in accordance with Article 769.

(2) Extracts of other COMSEC material (including keying material not marked CRYPTO) does not have to be documented on local custody forms. This material must be handled and accounted for based on its assigned classification in accordance with OPNAVINST 5510.1.

g. Return of Defective Extracts to NSA :

(1) If specifically authorized by NSA, defective extracts will be forwarded to NSA on a SF 153 as a local custody issue.

(2) Do not assign a TN to the SF 153 and do not send a copy of the SF 153 to DCMS.

(3) Retain your copy of the SF 153 for accountability documentation.

h. Destroying and Documenting Destruction of Extracts :

(1) Extracts of COMSEC keying material marked CRYPTO shall be destroyed in accordance with Chapter 5.

(2) Extracts from other COMSEC material shall be destroyed based on their assigned classification in accordance with OPNAVINST 5510.1.

(3) Destruction of COMSEC material extracts will be recorded on local destruction documents in accordance with Article 736.

(4) Use a local custody document to account for defective extract(s) of COMSEC material returned to NSA.

(5) Attach a copy of the local custody document to the local destruction record to account for an extract(s) returned to NSA when completing the destruction document for the entire edition.

787. ENTERING AMENDMENTS AND CORRECTIONS TO COMSEC PUBLICATIONS

a. General:

(1) Amendments and corrections are permanent changes to COMSEC and COMSEC -related publications (hereinafter referred to as publications) which incorporate up -to-date information.

(2) Actions based on outdated or incorrect information have the potential to adversely impact operational missions and administrative procedures. Therefore, amendments and corrections to publications must be entered only by properly trained and authorized personnel.

(3) The Custodian must ensure that written guidance, based on the procedures detailed in this article, is provided to all personnel entering amendments and corrections to publications.

(4) Changing a publication on the basis of an apparent discrepancy is not authorized. Changes to publications may be entered only as authorized by the publication's originator.

(5) Figure 7 -4 is a check -off list which may be reproduced for use in entering changes to COMSEC material and COMSEC -related publications and Figure 7 -5 is an example Certification of Amendment Entry form.

b. Types of Amendments:

(1) Printed Amendments:

(a) Printed amendments may consist of replacement pages, cut -out inserts, pen -and-ink changes, or any combination thereof.

(b) Printed amendments are, normally, distributed via the CMIOs or directly from DCMS.

(2) Message Amendments:

Message amendments normally consist only of pen - and-ink changes.

(3) Corrections to Amendments:

(a) Corrections to amendments are permanent alterations to printed or message amendments.

(b) Corrections may be printed or they may be issued as a message. Normally, the next printed amendment or message amendment will incorporate the information issued in a correction.

c. Numbering of Amendments and Corrections :

(1) All amendments to a basic publication are numbered consecutively while corrections to amendments are not numbered.

(2) Amendments and corrections to amendments must be recorded on the Record of Amendments (ROA) page of the publication. For example, the record of amendments and corrections to amendments entered in a specific publication could appear as follows: (printed) Amendment 1, (printed) Amendment 2, (message) Amendment 3, (Printed) Correction to Amendment 3.

(3) Amendments must be entered sequentially. For example, Amendment 4 may not be entered before Amendment 3 has been entered. In the event more than one correction to the same amendment is received, the corrections should be entered according to the date of promulgation.

d. Custodian Actions :

(1) Upon receipt, promptly review amendments and corrections and promulgate any significant information to appropriate command personnel.

(2) Next, the amendments and corrections will be entered as directed by originator.

(3) Custodians who transfer AL -4 publications to another CMS account must forward all amendments or corrections to the command(s) holding the basic publication for a period not to exceed 90 days. Thereafter, the recipient must coordinate with the CA to ensure receipt of future amendments.

e. Supply of Amendments :

(1) DCMS and the servicing CMIO of an account are responsible for supplying the command with printed amendments and corrections. However, the Custodian is responsible for ensuring that a publication contains the most current amendment. Status documents (e.g., CMSR) are the most up -to-date sources for determining the latest amendment to a COMSEC publication.

(2) Request disposition instructions from the originator for excess or unneeded copies of classified, accountable printed amendments and corrections. Ensure that the authorization for destruction and/or transfer is annotated on the SF 153 Transfer Report.

(3) Excess or unneeded copies of unclassified, non-accountable amendments and corrections may be destroyed at the discretion of the Custodian.

f. Local Custody:

Local custody issue of AL 1 or and AL 2 printed amendments and corrections must be documented on an appropriate local custody document.

g. Entering Amendments:

(1) Instructions:

(a) Each amendment provides instructions on the status or effective date of the amendment and step-by-step procedures for entering the amendment (e.g., specifically identifying which pages are to be removed from the basic publication and which pages from the amendment are to be added, and/or pen-and-ink corrections).

NOTE: Amendment instructions must be read and clearly understood prior to entering an amendment.

(b) Pen-and-Ink Changes:

(1) Only **black ink** will be used to make pen-and-ink corrections. No other color of ink may be used.

(2) Pen-and-ink corrections must be identified, in the margin, opposite their entry (e.g., Amend 5, Correction to Amend 5).

(c) Printed Changes:

(1) Effective amendments must be promptly entered and verified as soon as possible after receipt.

(2) An amendment effective in the future should be entered as close to its effective date as possible. If an amendment is entered substantially before its effective date, annotate "Effective (date)" in the margin of each replacement page and opposite each pen-and-ink change.

(2) Recording the Entry:

(a) The individual entering the amendment must sign and date the ROA Page of the publication certifying that he/she entered the change.

(b) The identity of the change (e.g., Amendment 1 or Correction to Amend 1) and, if applicable, the ALCOM number and/or DTG of the message, must be recorded on the ROA Page in order to properly identify the change.

(3) Entering Amendments in Sealed Publications :

If a sealed publication is opened to enter an amendment or a correction , the publication should be resealed after verification of the change and pagechecking the publication (if required).

(4) Pagecheck of Publication and Amendment Residue :

Conduct a pagecheck of publications and amendment residue in accordance with Article 757 and Annex Y. Ensure that the publication's Record of Pagechecks (ROP) Page is annotated.

(5) Verifying Proper Entry of an Amendment :

(a) The entry of amendments must always be verified by a second individual. Any properly cleared and authorized person (other than the individual who entered the amendment) may verify an amendment entry.

(b) The person verifying an amendment entry must certify, by placing their initials in the margin alongside the amendment entry on the ROA Page, that it was entered correctly and that the signature, date, and amendment identification have been entered on the ROA Page of the basic publication.

NOTE: Initialing the ROA Page entry is sufficient for verifying an amendment entry. A separate entry is not appropriate since the verifying individual did not actually enter the amendment.

(c) As a part of the verification process, the person verifying entry of an amendment must conduct a second pagecheck of the basic publication and amendment residue if the amendment removed, substituted, or added pages. This second pagecheck of the basic publication must be recorded (i.e., signature and date) as a separate entry on the ROP Page.

NOTE: The list of amendment residue, normally found at the end of the amendment instructions, must be used in pagechecking the amendment residue. The verifying individual must indicate this second pagecheck of the residue by initialing and dating the front page of the amendment residue.

h. Destruction of Amendment Residue :

Destruction of amendment residue may be verified in one of two ways at the option of the Custodian.

(1) Either the LH or User who signed the local custody document for the amendment can furnish the Custodian with a local destruction record and certification of proper entry and verification (see last page of this chapter); **OR**

(2) The Custodian can personally verify the entry by the LH or User, destroy the residue, and return the basic publication to the LH or User.

NOTE: 1. Classified amendment residue must be destroyed as soon as possible but no later than five working days after an amendment entry.
2. Unclassified amendment residue should be destroyed as soon as possible, but may be held and destroyed no later than five working days after the end of the month in which the amendment was entered.

i. Recording Destruction of Amendment Residue :

(1) Document destruction locally and maintain required records in accordance with Article 736.

(2) The destruction of unaccountable, classified amendment residue will be conducted in accordance with OPNAVINST 5510.1. Do not report destruction to DCMS.

790. PROCEDURES FOR DESTROYING COMSEC MATERIAL IN PAPER FORM

a. General:

(1) Custodians must ensure that all personnel who destroy COMSEC material follow the destruction criteria, reporting and documentation requirements, methods, and procedures in this manual.

(2) Attention to detail when destroying COMSEC material cannot be overstressed. Failure to follow proper procedures is one of the principle causes of COMSEC incidents and practices dangerous to security.

(3) Keying material marked or designated CRYPTO is the most sensitive item of COMSEC material. Therefore, the immediate, complete, and proper destruction of superseded keying material is of the highest importance.

(4) Prior to destroying any COMSEC material, verify, validate, and sight each item of material to be destroyed.

(5) The two individuals destroying COMSEC material are equally responsible for the timely and proper destruction of the material and the accuracy of the destruction document(s).

(6) Destruction criteria (i.e., timeframes and authorized methods) are contained in Chapter 5. Reporting and documentation requirements are detailed in Article 736. The information below details the steps to be followed by all personnel when destroying COMSEC material.

b. Verifying Status Information :

(1) The individuals conducting destruction of COMSEC material must ensure that the material to be destroyed is in fact superseded and/or authorized for destruction prior to actually destroying the material.

(2) Custodians are responsible for ensuring that the correct (i.e., most up -to-date) status information for COMSEC material is provided to all personnel destroying COMSEC material.

c. Verifying Short Title and Accounting Data :

(1) To verify accurately the material being destroyed against the destruction document, the individual responsible for destruction must read the short title(s) and accounting data of the material being destroyed to the witness.

(2) The witness must verify the accuracy and completeness of the entries on the destruction document.

(3) The witness must then read the short title(s) and accounting data of the material being destroyed to the individual responsible for destruction who then verifies the accuracy and completeness of the entries on the destruction document.

d. Timeliness of Destruction :

The two individuals destroying COMSEC material must ensure the complete physical destruction of the material being destroyed within the timeframes specified in Chapter 5.

e. Security Safeguards :

The two individuals responsible for destroying COMSEC material must strictly observe the following security safeguards when the use of burnbags or other containers is required due to a large quantity of material being destroyed.

(1) Sealing and Marking Destruction Containers :

After verifying the material to be destroyed against the destruction record, place the material in burnbags or other destruction containers, seal them securely, and mark the containers to identify them as containing COMSEC material. In addition, the containers must be numbered to reflect the total number of containers (e.g., 1 of 3, 2 of 3, 3 of 3).

(2) Separation and Control of Destruction Containers :

(a) Keep all destruction containers which contain unshredded COMSEC material separate from all destruction containers containing non -COMSEC material. Until they are physically destroyed by an authorized method, destruction

containers containing unshredded COMSEC material must be afforded the security and storage protection required for the COMSEC material.

(b) Destruction containers containing strip -shredded COMSEC material must be protected based on the highest classification of the shredded material contained therein.

(c) Destruction containers containing cross -cut shredded paper COMSEC material may be treated as unclassified material.

(d) Destruction containers containing cross -cut shredded microfiche material must be protected based on the highest classification of the material.

NOTE: Depositing superseded COMSEC keying material segments or extracts into a burnbag, a special access control container (SACC) or other locked container does **not** constitute physical destruction. If a SACC is used, all deposited superseded keying material must be destroyed within the timeframes specified in Chapter 5.

(3) Transportation of Containers :

Transport destruction containers directly from the secure area to the area in which physical destruction will take place. Attending to other business or to personal matters while enroute to the destruction site is strictly prohibited .

f. Witnessing Destruction :

(1) The two individuals conducting destruction of COMSEC material must not complete (i.e., sign and date) destruction documents until after the material has actually been destroyed. Therefore, the two individuals conducting the destruction must personally witness the complete destruction of the material.

(2) In the case of large destruction facilities (e.g., disintegrators), operated for the benefit of commands in the area, the destruction containers may be given to the individual(s) who are operating the destruction facility. However, the two persons responsible for the destruction must physically sight the destruction container(s) being placed in the device by the operators.

NOTE: If a discrepancy in a COMSEC material destruction container is noted **prior to** the physical destruction of the container (e.g., inaccurately numbered or missing container, broken container) and if the nature of the container discrepancy causes any doubt whatsoever about the accuracy of the corresponding destruction document(s), then the contents of all containers involved must be removed and reverified.

g. Inspecting Destruction Devices and Destroyed Material :

(1) When an incinerator is used for destruction, ensure that the flues are properly screened and secured to prevent the escape of partially burned material.

(2) The two individuals conducting destruction must monitor the entire destruction process and inspect the destruction device and the surrounding area afterward to ensure that destruction was complete and that no material escaped during the destruction process. These procedures apply to all destruction devices discussed in Chapter 5.

(3) The residue from destroyed material must be inspected to ensure that the destruction was complete (i.e., no unburned and readable bits of material remain).

(a) In the case of shredders, choppers, and pulverizers (dry process), and pulpers and disintegrators (wet process), only a representative sample of the residue needs to be examined to ensure that the device was working properly.

(b) In the case of ash residue from an incinerator or other method of burning, the ashes must be inspected and, if necessary, broken up by carefully stirring or sifting, or be reduced to sludge with water.

793. U.S. ARMY AND AIR FORCE CMS ACCOUNTS

When corresponding with an Army (5XXXXX) or Air Force (6XXXXX) CMS account, the COR of that service must be an information addressee on all correspondence (e.g., letter, message). COR addressees are contained in Annex S.

CONFIDENTIAL (When Filled In)

CMS-25 ONE-TIME KEYING MATERIAL DESTRUCTION REPORT

Retain this form locally IAW Annex T, CMS 1. See Chapter 7, Art 790 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 #	Date Extracted	Date Destroyed	Signature	Signature

CMS 1

CONFIDENTIAL (When filled in)

Explanation of Keytape Crypto Periods

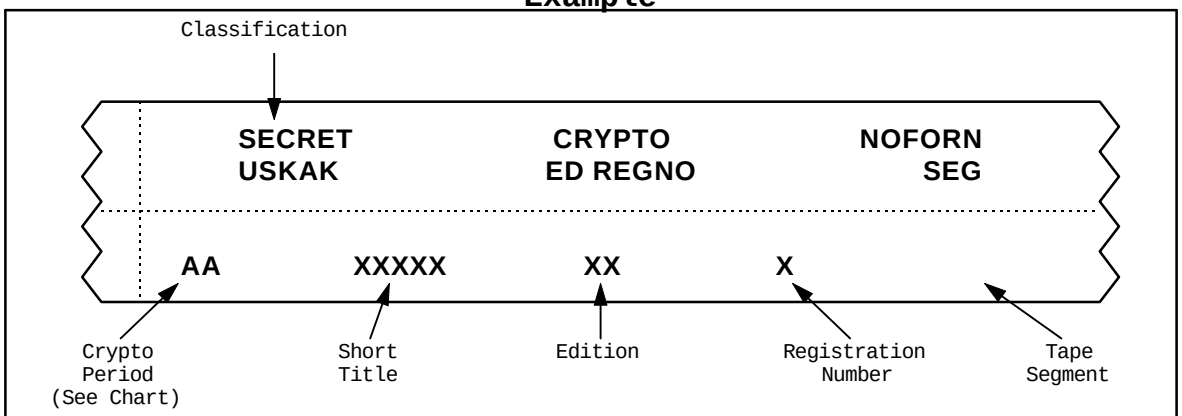
Number of Tape Segments

First Letter	# of Keys	# of Copies of Keys	Total Segments
A	31	1	31
B	5	3	15
C	1	5	5
D	6	5	30
E	5	1	5
F	1	10	10
G	16	1	16
H	1	31	31
I	1	15	15
J	26	1	26
L	35	1	35
M	2	1	2
N	(Contact Controling Authority)		
Q	34	1	34
S	75	1	75
T	12	1	12
U	65	1	65
V	62	1	62
W	1	65	65
R	4	5	20
Y	26	2	52
Z	15	5	75

When to Change

Second Letter	Crypto Period
A	Daily (24 Hours)
B	Weekly (7 Days)
C	Monthly
D	Special (≤ 24 Hours)
E	No Prescribed Period
F	Three Months
G	Yearly
H	(Contact Controlling Authoyity)
I	Six Months
J	Monthly (Beginning 1st Day Used)

Example



NOTE: See Figure 2-1 for additional explanation of Crypto Keytape Periods

CLASSIFIED BY CMS-1

CONFIDENTIAL (When filled in)

FIGURE 7-1

CMS 25 ONE-TIME KEYING MATERIAL DESTRUCTION REPORT

1. **Purpose:** The CMS 25 COMSEC keying material report is a two-sided document used to record destruction of individual, one-time keying material segments of COMSEC material. Side one is numbered 1-31. The reverse side provides an explanation for the digraphs that are printed to the left of the short title on each segment of extractable tape.

2. **Preprinted CMS 25 Reports:** The current version of the CMS 25 (revised date of 11/82) or a locally prepared equivalent form may be used.

3. **Date of Extract:** This column is used to record the actual date an individual segment of extractable COMSEC keying material is extracted from its protective packaging. The use of this column is optional.

4. **Signatures:** The two individuals conducting destruction shall affix their signatures or initials directly opposite the segment being destroyed. The use of lines or ditto marks to connect signatures or initials is **prohibited**.

5. **Date of Destruction:** The actual date of destruction must be entered opposite the two sets of signatures or initials. The use of lines or ditto marks to connect dates is **prohibited**.

6. **Account/Short Title Date:** The complete short title, edition, register or serial number (if applicable), and AL code must be annotated on the bottom of this report.

7. **Improperly Completed Form:** The lack of two signatures or sets of initials and a date of destruction for each copy of segmented material destroyed is a PDS. The absence of or lack of a complete short title, edition, register/serial number and AL code constitutes a PDS. Handle PDSs in accordance with Chapter 10.

8. **Restrictions on Use:** When the CMS 25 or a locally prepared equivalent form is used, the destruction of one and only one copy of a short title may be recorded on the report.

FIGURE 7-1

CMS 25B COMSEC KEYING MATERIAL LOCAL DESTRUCTION REPORT

The individuals whose signatures appear below certify that they have destroyed the individual keytape segments on the dates indicated. Retain this form in accordance with Annex T.

CONFIDENTIAL (When filled in)

Seg	Signature	Signature	Date of Destruction
1A			
2A			
3A			
4A			
5A			
6A			
7A			
8A			
9A			
10A			
11A			
12A			
13A			
14A			
15A			
16A			
17A			
18A			
19A			
20A			
21A			
22A			
23A			
24A			
25A			
26A			
27A			
28A			
29A			
30A			
31A			

_____
(Command Title and Account Number)

_____	_____	_____	_____
SHORT TITLE	EDITION	REG #	AL CODE

Classified by: CMS 1
Declassify on: Originating Agency's Determination Required

CONFIDENTIAL (When filled in)

FIGURE 7-2

CMS 25B COMSEC KEYING MATERIAL LOCAL DESTRUCTION REPORT

The individuals whose signatures appear below certify that they have destroyed the individual keytape segments on the dates indicated. Retain this form in accordance with Annex T.

CONFIDENTIAL (When filled in)

Seg	Signature	Signature	Date of Destruction
1B			
2B			
3B			
4B			
5B			
6B			
7B			
8B			
9B			
10B			
11B			
12B			
13B			
14B			
15B			
16B			
17B			
18B			
19B			
20B			
21B			
22B			
23B			
24B			
25B			
26B			
27B			
28B			
29B			
30B			
31B			

_____
(Command Title and Account Number)

_____ _____ _____ _____
SHORT TITLE EDITION REG # AL CODE

Classified by: CMS 1
Declassify on: Originating Agency’s Determination Required

CONFIDENTIAL (When filled in)

FIGURE 7-2

CMS 25B COMSEC KEYING MATERIAL LOCAL DESTRUCTION REPORT

1. **Purpose:** The CMS 25B is a two-sided document used to record destruction of keytape segments of COMSEC keying material packaged in the "VF" format (62 unique segments per canister). The destruction of segments 1-31A shall be recorded on the "A" side. Segments 1-31B on the "B" side. Complete information must be recorded on both sides when this form is used.

2. **Signatures:** The two individuals conducting destruction shall affix their signatures or initials directly opposite the segment being destroyed.

3. **Date of Destruction:** The actual date of destruction must be entered opposite the two sets of signatures or initials.

4. **Account/Short Title Data:** The CMS account number of the issuing account must be annotated on the CMS 25B in addition to the complete short title, edition, register or serial number (if applicable), and the AL code. CMS Users and LHs of a command other than the issuing command must annotate their command title vice the title of the issuing command.

5. **Improperly Completed Form:** The lack of two signatures or sets of initials and a date of destruction for each copy of segmented material destroyed is a PDS. The absence of or lack of a complete short title, edition, register/serial number, and AL code constitutes a PDS. Handle PDSs in accordance with Chapter 10.

FIGURE 7-2

CMS 25C COMSEC KEYING MATERIAL LOCAL DESTRUCTION REPORT

The individuals whose signatures appear below, certify that they have destroyed the individual keytape segments on the dates indicated. Retain this form in accordance with Annex T.

CONFIDENTIAL (When filled in)

Seq/Copy #		Signature	Signature	Date of Destruction	
1/01					
1/02					
1/03					
1/04					
1/05					
2/01					
2/02					
2/03					
2/04					
2/05					
3/01					
3/02					
3/03					
3/04					
3/05					

_____
(Command Title and Account Number)

SHORT TITLE _____ **EDITION** _____ **REG #** _____ **AL CODE** _____

Classified by: CMS 1
Declassify On: X1

CONFIDENTIAL (When filled in)

FIGURE 7-3

CMS 25MC COMSEC KEYING MATERIAL LOCAL DESTRUCTION REPORT

1. **Purpose:** The CMS 25MC is used to record destruction of multiple copy segments (i.e., 1/01, 1/02, 1/03, etc.) of COMSEC keying material packaged in canisters.

2. **Signatures:** The two individuals conducting destruction must affix their signatures or initials in the signature blocks dirrectly opposite the specific copy of the segmented keying material being destroyed.

3. **Date of Destruction:** The actual date of destruction must be annotated in the date of destruction block.

4. **Account/Short Title Data:** The CMS account number of the issuing account command, the complete short title, edition, register or serial number (if applicable), and the AL code must be annotated on this form. CMS Users and LHs of a command other than the issuing command must annotate their command title vice the title of the issuing command.

5. **Improperly Completed Form:** The lack of two signatures or sets of initials and a date of destruction for each copy of segmented material destroyed is a PDS. The absence of or lack of a complete short title, edition, register/serial and AL code constitutes a PDS. Handle PDSs in accordance with Chapter 10.

FIGURE 7-3

CHECK-OFF LIST FOR ENTERING AMENDMENTS TO PUBLICATIONS

Initial Each Item When Completed

Verifying	Person Entering Amendment (Initial)	Person Entry (Initial)
1. Instructions for entering the change have been read and understood.	_____	_____
2. Black ink only used for deletions and pen-and-ink changes.	_____	_____
3. Prepared cutouts used. Locally-typed cutouts identify change being entered (e.g., Amend 1).	_____	_____
4. Information superseded by a cutout deleted in ink before cutout affixed.	_____	_____
5. Flaps used only if there is no room to affix cutout flat on page.	_____	_____
6. Each pen-and-ink change is identified by amendment number or correction to a specific amendment.	_____	_____
7. For change entered substantially before its effective date, "Effective (date)" notation marked in margin on all pages where change was made.	_____	_____
8. Record of Amendments page completed and signed by the person entering the change and initialed by the person who verified the entry.	_____	_____

FIGURE 7-4

CHECK-OFF LIST FOR ENTERING AMENDMENTS TO PUBLICATIONS

Initial Each Item When Completed

	Person Entering Amendment (Initial)	Person Verifying Entry (Initial)
9. If change removed, added, or substituted pages, publication pagechecked and the Record of Pagechecks page signed and dated by person who entered the change and the person who verified the change.	_____	_____
10. If residue from change is more than one page, pagecheck of residue made and residue initialed or signed and dated by the person who entered the change and the person who verified the change.	_____	_____
11. Residue of change entered by LH Custodian or User was destroyed. Date of destruction and signatures of the two people who destroyed the material recorded on local destruction record, and record forwarded to the Custodian.	_____	_____

_____ (Date and signature of person who entered the change)

_____ (Date and signature of person who verified the change)

FIGURE 7-4

MEMORANDUM

_____
(date)

From:
To: CMS Custodian

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

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

1. On (date), Amendment _____, accounting number _____, was entered into (publication short title and edition), accounting number _____.

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

3. The residue of the amendment was properly destroyed (date) by the two individuals whose signatures appear below:

_____ _____
(Signature) (Signature)

_____
(Signature)

EXAMPLE OF CERTIFICATION OF AMENDMENT ENTRY

FIGURE 7-5

CHAPTER 8 - DISESTABLISHMENT OF A CMS ACCOUNT

CHAPTER 8 - DISESTABLISHMENT OF A CMS ACCOUNT

801. REQUIREMENT TO DISESTABLISH A CMS ACCOUNT

a. A CMS account must be disestablished whenever the account command is being disestablished or a command no longer requires COMSEC material. The requirement to disestablish a CMS account will be validated by the action addressees indicated in Article 805.

b. Due to the considerable workload involved, disestablishing and later reestablishing a CMS account is generally not practicable for ships undergoing overhaul except when the yard period will exceed one year or for Marine Corps commands undergoing reorganization or a temporary stand -down.

NOTE: THE PROVISIONS OF THIS CHAPTER APPLY ONLY TO NUMBERED OR PARENT CMS ACCOUNTS. THE PARENT CMS ACCOUNT MUST DIRECT LOCAL HOLDERS AND USERS IN THE DISESTABLISHMENT OF THEIR HOLDINGS AND TERMINATION OF ANY SUPPORT AGREEMENTS.

805. DISESTABLISHMENT PROCESS

a. **Lead Time to Disestablish:** A request to disestablish a CMS account must be submitted at least 60 days prior to the date the command desires to disestablish.

b. **Request to Disestablish:** A letter or message request to disestablish a CMS account must be forwarded as indicated below. Letters must be signed by the Commanding Officer or "Acting" Commanding Officer. (NOTE: Correspondence signed "By direction" is not acceptable.) Address a CMS account disestablishment request as follows:

(1) Navy afloat commands :

Submit to CINCLANTFLT or CINCPACFLT, as applicable, info DCMS//30//, NISEEAST DET NORFOLK VA//526CS/635SB, NISEEAST CHARLESTON SC//40C//, DIRNSA//Y181//, CMIO, and the administrative Chain of Command.

(2) Navy shore and all MSC commands:

Submit to ISIC, info DCMS//30//, DIRNSA//Y181//, NISEEAST DET NORFOLK VA//526CS/635SB//, NISEEAST CHARLESTON SC//40C//, servicing CMIO and the administrative Chain of Command.

(3) Marine Corps commands:

Submit to Commandant, Marine Corps//CSB//, info DCMS//30//, DIRNSA//Y181//, NISEEAST DET NORFOLK VA//526CS/635SB, NISEEAST CHARLESTON SC//40C//, CMIO, and the administrative Chain of Command.

(4) Coast Guard commands :

Submit to COGARD TISCOM//OPS4//, info COMLANTAREA or COMPACAREA COGARD, DCMS//30//, NISEEAST DET NORFOLK VA//526CS/635SB//, NISEEAST CHARLESTON SC//40C//, CMIO Norfolk and/or DCS station, and the administrative Chain of Command. (R

(5) Naval Reserve commands :

Submit to COMNAVRESFOR//01D//, info DCMS//30//, NISEEAST DET NORFOLK VA//526CS/635SB//, NISEEAST CHARLESTON SC//40C//, CMIO Norfolk and/or DCS station, and the administrative Chain of Command. (R

c. DCMS Action : Upon approval by applicable authority to disestablish a CMS account, DCMS will:

(1) Provide to the command an inventory of COMSEC material currently held and in -transit (IT), and disposition instructions for this material.

(2) Provide to the command and their ISIC a copy of the command's current inventory and material IT.

(3) Provide the account disposition instructions for all COMSEC accounting records and CMS -related files.

(4) Notify CMIO Norfolk to stop automatic distribution of COMSEC material. (R

(5) Send final clearance to the account command and/or their ISIC and the cognizant CMS A&A Training Team Command upon DCMS verification that all COMSEC material has been disposed of properly.

810. INVENTORY REQUIREMENT

a. An inventory must be conducted as part of the disestablishment process. Upon receipt of a disestablishment request, DCMS will forward an inventory which reflects all account transactions and holdings as of the date in the heading of the SF 153. (R

b. Upon receipt of the inventory, line -out the type of inventory in the heading and replace it with "disestablishment." The inventory must be completed and returned to DCMS a minimum of 10 working days prior to the requested disestablishment date.

815. DISPOSITION OF COMSEC MATERIAL

a. All COMSEC material must be disposed of in accordance with the directions provided by DCMS. Marine Corps accounts will receive disposition instructions for their equipment assets from their ISIC.

NOTE: Disposition instructions received via phone are UNOFFICIAL and must NOT be executed until official written documentation is received.

b. Unsealed keying material, maintenance manuals, operating manuals, amendments, and resealed keying material must be pagechecked prior to transfer or destruction. Additionally, maintenance and repair kits must have all components inventoried prior to transfer or destruction. Any discrepancies must be reported in accordance with Annex X.

c. Disposition accounting reports (e.g., transfer or destruction) must be completed and forwarded in accordance with Chapter 7.

d. The running inventory (R/I) must clearly and accurately contain a TN number in the disposition column which corresponds to the disposition of all AL 1 and AL 2 material (and AL 4 when transferred the CMIO, cache, or non -DON account). Annotate the date and disposition for all other material not being disposed (R of under a TN in the disposition column.

820. DISPOSITION OF RECORDS

a. Commands **not** being disestablished/decommissioned :

(1) Retain all CMS account records and CMS -related files until final clearance has been received. Upon receipt of the final clearance, destroy all CMS -related files and account records.

(2) Retain the final clearance message from DCMS for one year and inform CMS Custodian and Alternate(s) that the final clearance has been received.

b. Commands being disestablished/decommissioned :

(1) Commands that are being disestablished/decommissioned prior to receipt of the final clearance message must forward all CMS -related files and account records to their ISIC.

(2) Commands **not** disestablished/decommissioned prior to receipt of the final clearance message must, upon receipt of the final clearance message from DCMS, destroy all CMS -related files and account records. Retain the final clearance message for one year.

825. **DISESTABLISHMENT REPORT**

a. The CMS account command, as the final step in disestablishing a CMS account, must send a disestablishment report to DCMS//30//, info to the administrative Chain of Command, and keying material controlling authorities.

(1) Submission of this report indicates that all COMSEC material has been properly disposed of and that account records are up -to-date and correct.

(2) The ISIC must su bmit the disestablishment report for commands that were disestablished/decommissioned prior to receipt of the final clearance message.

b. The disestablishment report shall state that the COMSEC material was properly disposed of in accordance with DCMS and/or Marine Corps ISIC disposition instructions. Further, the disestablishment report shall give the future addresses and telephone numbers of the Commanding Officer and the CMS Custodian, and, if the command is being disestablished, shall specify the ISIC to whom the required account records were forwarded.

830. RESPONSIBILITIES OF IMMEDIATE SUPERIOR IN COMMAND (ISIC)

a. ISICs are responsible for validating the requirement to disestablish a CMS account prior to the CMS account command being disestablished by DCMS.

b. ISICs should make every effort to verify that all accountable COMSEC material has been properly disposed of and that the applicable documentation supporting material disposition has been correctly prepared and forwarded to DCMS. Any discrepancies discovered by DCMS during the disestablishment review (for commands already disestablished/decommissioned) must be resolved by the ISIC of the disestablishing account.

c. Retain CMS records for disestablished/decommissioned CMS account commands until DCMS forwards the final clearance message. After receipt of the final clearance message, destroy all records and maintain the final clearance message for one year.

d. Submit disestablishment report for account commands that were disestablished/decommissioned prior to receipt of the final clearance message from DCMS.

835. SUMMARY OF STEPS REQUIRED TO DISESTABLISH A CMS ACCOUNT (R

a. Coordinate with applicable authority for disestablishing the account (See Article 805.b.).

b. Submit request to disestablish.

c. Conduct an inventory, and dispose of COMSEC material as directed by DCMS and/or ISIC for Marine Corps accounts.

d. Complete and submit disposition documentation to DCMS for AL 1 and 2 material (and AL 4 when transferred the CMIO, cache, or non -DON account). (R

e. Annotate the TN in the disposition column of the R/I for each item of AL 1 and 2 material (and AL 4 when transferred the CMIO, cache, or non -DON account). (R

f. Annotate date and disposition in the disposition column of the R/I for all material not disposed of under a TN.

g. Dispose of applicable CMS account records as directed by DCMS. Commands not disestablished/decommissioned must retain final clearance message for one year.

h. Submit account disestablishment report to addressees in Article 825.

CHAPTER 9 - COMSEC INCIDENT REPORTING

CHAPTER 9 - COMSEC INCIDENT REPORTING

Figures :

901. INTRODUCTION TO THE NATIONAL COMSEC INCIDENT REPORTING AND EVALUATION SYSTEM (NCIRES)

a. General: To some degree, every item of COMSEC material is accounted for and controlled because of the role it plays in the cryptographic processes that protect or authenticate U.S. Government information transmitted electrically. To counter the threat posed to secure communications by COMSEC material mishandling, losses, or thefts, the National Security Agency (NSA) established the National COMSEC Incident Reporting and Evaluation System or NCIRES.

b. Purpose: The NCIRES serves primarily to ensure that all reported incidents involving COMSEC material are evaluated so that actions can be taken to minimize their adverse impact on national security. The NCIRES is comprised of NSA, the heads of departments or agencies, material controlling authorities (CAs) and equipment resource managers. Within the DON, the incident reporting and evaluation system also includes Closing Action Authorities (CAAs). An explanation of each and their roles in COMSEC incident reporting follows.

905. NATIONAL SECURITY AGENCY (NSA)

In support of the NCIRES, NSA established and maintains a national COMSEC Incident Trend Analysis (CITA) data base, providing national trend analysis reports to departments and agencies to promote COMSEC awareness and remedial action. In addition, NSA directs supersession of compromised future keying material that has not reached the user account and evaluates:

a. CRYPTOGRAPHIC incident reports,

b. PERSONNEL incident reports, and

c. PHYSICAL incident reports involving:

(1) Keying material where the CA cannot be identified.

(2) Multiple CAs of more than one department, agency, or organization.

(3) Suspected or known tampering; sabotage; evidence of covert penetration of packages; evidence of unauthorized or unexplained modifications to COMSEC equipment, security containers, or vaults where COMSEC material is stored; and COMSEC material other than keying material (e.g., documents, algorithms, logic).

910. DIRECTOR, COMMUNICATIONS SECURITY MATERIAL SYSTEM (DCMS)

Within the NCIRES, the NSA has established COMSEC Incident Monitoring Activities (CIMA). Each service has its own monitoring activity. As the DON CIMA, DCMS is responsible to:

a. Establish procedures to ensure that COMSEC material incidents are reported promptly to the specified authorities.

b. Evaluate PHYSICAL COMSEC incidents involving:

(1) Two or more CAs and they are all DON.

(2) One DON CA when the CA caused the incident, except as otherwise noted.

(3) Losses of Two -Person Integrity (TPI) involving Secret and/or Confidential keying material marked or designated CRYPTO.

c. Determine when a reported COMSEC incident should be considered a COMSEC insecurity.

d. Establish data bases in support of the national CITA data base.

915. MATERIAL CONTROLLING AUTHORITY (CA)

Controlling authorities (CAs) are responsible for directing the establishment and operation of a cryptonet/circuit and managing the operational use and control of keying material assigned to a cryptonet/circuit. In the context of COMSEC incident reporting and evaluation, the CA will normally evaluate reports of PHYSICAL incidents involving his/her material, except as otherwise noted in this chapter. COMSEC material CAs may be found in CMSR.

920. DEPARTMENT OF THE NAVY (DON) RESOURCE MANAGERS

a. DON Resource Managers perform and coordinate DON service planning and funding for designated COMSEC material resources. Within the DON, COMNAVCOMTELCOM and DCMS serve as resource managers for certain paper COMSEC material and material -related items.

b. CNO is the DON resource manager for COMSEC equipment. For the purpose of distribution analysis and planning, CNO

conducts appropriate consultation and coordination with COMNAVCOMTELCOM and DCMS.

c. To effectively manage COMSEC material resources, COMNAVCOMTELCOM//N32/N3/N3X// and DCMS//20// must be included as action or information addressees on COMSEC incident reports as required by this chapter.

925. CLOSING ACTION AUTHORITY (CAA)

An administrative senior or other designated command that reviews details of incidents or insecurities reported by the commands and activities for which he/she is responsible. The CAA determines the need for further actions and reporting. See Article 955 for identification and responsibilities of CAAs.

930. GUIDANCE ON COMSEC INCIDENT REPORTING

a. General:

(1) To be effective, the NCIRES must receive prompt and clear information relating to the circumstances surrounding an incident. This information is critical to the rapid initiation of appropriate damage limitation or recovery measures by the evaluating authority.

(2) Reports of any incident must be made irrespective of the judgment of the CMS Custodian or his/her supervisor as to whether or not an incident or possible incident occurred.

b. Disciplinary action: Disciplinary action should **not** be taken against individuals for reporting a COMSEC incident unless the incident occurred as the result of willful or gross neglect by those individuals.

c. Applicability: The COMSEC incident reporting requirements of this chapter apply to these COMSEC materials:

(1) Classified and unclassified COMSEC keying material marked or designated CRYPTO (includes electronic key converted from NSA-produced tape key and field-generated electronic key generated from a KG-83 or KGX-93, for example).

(2) Controlled Cryptographic Item (CCI) equipment.

(3) Classified COMSEC equipment.

(4) Classified COMSEC -accountable maintenance manuals, operating instructions, and publications.

d. Unclassified COMSEC material :

Report incidents involving unclassified non-CCI equipment and related devices, unclassified publications, manuals, operating instructions, and unclassified key **not** marked or designated CRYPTO in accordance with Chapter 10.

e. JCS-Positive Control material :

Report incidents involving JCS -positive control Nuclear Command and Control (i.e., SAS (Sealed Authenticator System) two-person controlled) material in accordance with CJCSI 3260.1. (R

f. NATO material :

Report incidents involving COMSEC material designated for NATO use in accordance with AMSG -293.

g. Classification and transmission :

(1) Classify incident reports according to content of the message or letter text. Mark unclassified reports For Official Use Only (FOUO).

(2) Submit reports in message format via the General Service (GENSER) AUTODIN Communications Network. Use facsimile **or** mail only when a message cannot be submitted.

(3) Initial and amplifying message reports are excluded from MINIMIZE restrictions.

h. How to use this chapter to report a COMSEC incident :

Article to Review:

(1) Determine whether the COMSEC incident reporting requirements of this chapter apply to the COMSEC material in question. For example, incidents involving unclassified equipment (not designated CCI) are reportable in accordance with Chapter 10. **930**

Article to Review:

(2) Determine the type or category of COMSEC incident being reported (i.e., CRYPTOGRAPHIC, PERSONNEL, and/or PHYSICAL). This will help determine action and information addressees (see subparagraph (4) below). **945**

(3) Determine the types of COMSEC incident report that may be required of you. These articles also outline report precedence, timeframes, format, content, and classification requirements. **950 960 965 & 975**

(4) Determine initial and amplifying report addressees. **970**
Note how the incident category, type of COMSEC material involved, controls it (or promulgates it) dictates report action and information addressees.

(5) Determine whether the incident you are reporting **935**
requires anaccounting adjustment.

(6) What is a final letter report? When m ight one be **975**
required of your command, and who may require it?

(7) Finally, use the COMSEC Incident Report Format/Content Checklist in Figure 9 -1 at the end of this chapter. It will help you verify that you have supplied all of the information required for a swift evaluation. An example final letter report associated with COMSEC incident reporting is shown in Figure 9-2 at the end of this chapter to further assist you.

935. SUBMISSION REQUIREMENTS FOR SF 153 RELIEF FROM ACCOUNTABILITY AND POSSESSION ACCOUNTING REPORTS

In addition to submitting an incident message report, commands that report the loss or finding of COMSEC material may also be required to submit one of these accounting reports. Completion instructions for both reports are outlined in Article 739, 745 and Annex V. Specific guidance on when each is required follows:

a. An SF 153 **Relief from Accountability Report** must be submitted whenever a whole edition, complete short title, or separately accountable end item of AL 1 or AL 2 material is missing **and** no documentation exists which indicates that the item was either transferred or destroyed. Failure to submit this accounting report when required will result in the missing item continuing to be charged to an account in the DCMS COR data base.

NOTE: The loss of individual segments, pages of manuals, or equipment items accounted for only as components of an end item must be reported in accordance with Annex X.

b. An SF 153 **Possession Report** must be submitted whenever a whole edition, complete short title, or separately accountable end item of AL 1 or AL 2 material comes into the possession of an account and either of the following is true:

(1) There is no documentation that the found material was ever held by or charged to the account, **OR**

(2) The material was previously held by the account but properly documented as having been transferred or lost, and lined out on the running inventory.

(3) Do not submit an SF 153 Possession Report whenever a whole edition, complete short title, or separately accountable AL 1 or AL 2 material is found that was documented as destroyed and reported to DCMS as destroyed, but follow these instructions:

(a) Report the finding of the material as a PHYSICAL incident in accordance with Article 945.

(b) If the material is authorized for destruction, destroy it and document the actual destruction locally. Indicate in the report of the incident that the found material was destroyed.

(c) If the found material is not authorized for destruction (e.g., found material is equipment or future key that was previously reported as "prematurely" destroyed), request disposition instructions in the incident report.

940. REPORT SUBMISSION GUIDANCE

a. Incidents will normally be reported by the unit that detected the incident. The unit that detected the incident may or may not be the unit that caused the incident. For example, incidents involving the use of a non -approved transportation method to ship COMSEC material are most often reported by the recipients of such shipments as opposed to the originators.

b. When an incident occurs at the LH command leve l, exactly who reports the incident is up to the CMS account command. The CMS account command must ensure that the locally prepared CMS instruction it issues to its LH(s) clearly outlines who is responsible to report these occurrences and how they are to be reported.

c. When the Commanding Officer of a LH command is not the same as the Commanding Officer of the CMS account command, the CMS account command must clearly spell out the incident reporting responsibilities in its LOA. (NOTE: Annex L contains a sample LOA with the minimum requirements to be addressed.)

d. The activity that reports an incident will add its servicing A&A team as an information addressee to all initial and amplifying reports.

945. CATEGORIES AND EXAMPLES OF COMSEC INCIDENTS

a. General: The incident listing herein is not all inclusive. Additional reportable incidents that may be unique to a given cryptosystem, or to an application of a cryptosystem, will be listed in the operating instructions and maintenance manuals for that cryptosystem. Accordingly, each command must ensure that these documents are reviewed during COMSEC incident/insecurity familiarization training.

b. COMSEC incidents are divided into **three** categories:

(1) **Cryptographic**,

(2) **Personnel**, and

(3) **Physical**.

NOTE: Representative types of incidents for each category are provided in the paragraphs that follow.

c. Examples of Cryptographic Incidents :

(1) Use of COMSEC keying material that is compromised, superseded, defective, previously used (and not authorized for reuse), or incorrect application of keying material; such as:

(a) Use of keying material that was produced without the authorization of NSA (e.g., homemade maintenance, DES key, or codes).

NOTE: NSA authorization to generate key in the field is implicit in the publication of operating instructions for cryptosystems which possess that capability.

(b) Use, without NSA au thorization, of any keying material for other than its intended purpose.

(c) Unauthorized extension of a cryptoperiod.

(2) Use of COMSEC equipment having defective cryptographic logic circuitry, **or** use of an unapproved operating procedure; such as:

(a) Plaintext transmission resulting from a COMSEC equipment failure or malfunction.

(b) Any transmission during a failure, or after an uncorrected failure that may cause improper operation of COMSEC equipment.

(c) Operational use of equipment w ithout completion of required alarm check test or after failure of required alarm check test.

(3) Use of any COMSEC equipment or device that has not been approved by NSA.

(4) Discussion via nonsecure telecommunications of the details of a COMSEC equipment failure or malfunction.

(5) Any other occurrence that may jeopardize the cryptosecurity of a COMSEC system.

d. Examples of Personnel Incidents :

(1) Known or suspected defection.

(2) Known or suspected espionage.

(3) Capture by an enemy of persons who have detailed knowledge of cryptographic logic or access to keying material.

(4) Unauthorized disclosure of information concerning COMSEC material.

(5) Attempts by unauthorized persons to effect disclosure of information concerning COMSEC material.

NOTE: For COMSEC purposes, a personnel incident does not include instances of indebtedness, spousal abuse, child abuse, substance abuse, or unauthorized absence (when there is no material missing or reason to suspect espionage or defection).

e. Examples of Physical Incidents :

(1) The physical loss of COMSEC material. Includes whole editions as well as a classified portion thereof (e.g., a classified page from a maintenance manual, keytape segment). (**NOTE:** If a record of destruction is required but is not available, the material must be considered lost.)

(2) Unauthorized access to COMSEC material by uncleared persons.

(3) Unauthorized access to COMSEC material by persons inappropriately cleared.

(4) COMSEC material discovered outside of required accountability or physical control; for example:

(a) Material reflected on a destruction report as having been destroyed and witnessed, but found not to have been destroyed.

(b) Material left unsecured and unattended where unauthorized persons could have had access.

(c) Failure to maintain required TPI for classified keying material, except where a waiver has been granted.

(5) COMSEC material improperly packaged or shipped.

(6) Receipt of classified equipment, CCI equipment, or keying material marked or designated CRYPTO with a damaged inner wrapper.

(7) Destruction of COMSEC material by other than authorized means.

(8) COMSEC material not completely destroyed and left unattended.

(9) Actual or attempted unauthorized maintenance (including maintenance by unqualified personnel) or the use of a maintenance procedure that deviates from established standards.

(10) Tampering with, or penetration of, a cryptosystem; for example:

(a) COMSEC material received in protective packaging (e.g., key tape canisters) which shows evidence of tampering.

(b) Unexplained (undocumented) removal of keying material from its protective technology.

(c) Known or suspected tampering with **or** unauthorized modification of COMSEC equipment.

(d) Discovery of a clandestine electronic surveillance or recording device in or near a COMSEC facility.

(e) Activation of the anti-tamper mechanism on, or unexplained zeroization of, COMSEC equipment when other indications of unauthorized access or penetration are present.

NOTE: 1. Hold information concerning tampering with COMSEC equipment, penetration of protective technologies, or clandestine devices on a strict need-to-know basis. Immediately and simultaneously report to NSA//Y264//, Article 970.
2. When tampering or penetration is known or suspected, wrap and seal the material along with all protective secure, limited-access storage available. The until further instructions are received from NSA.
3. Where a clandestine surveillance or recording device is suspected, do not discuss it in the area of the device. Take no action that would alert the COMSEC exploiter, except on Instructions from the applicable counterintelligence organization or NSA. Take no action that would jeopardize potential evidence.

(11) Unauthorized copying, reproduction, or photographing of COMSEC material.

(12) Deliberate falsification of COMSEC records.

(13) Any other incident that may jeopardize the physical security of COMSEC material.

950. TYPES OF COMSEC INCIDENT REPORTS & SUBMISSION REQUIREMENTS

a. There are **four** types of incident reports:

(1) **Initial**,

(2) **Amplifying**,

(3) **Final**, and

(4) **Interim**.

b. **Initial:**

Submit this report for each COMSEC Incident. If all facts regarding the incident are included in the initial report, it may be accepted as a final report by the appropriate Closing Action Authority (CAA) identified in Article 955.

c. **Amplifying:**

Submit this report whenever significant new information is discovered or is requested by the evaluating authority. This report may also serve as a final report, if so accepted by the appropriate CAA.

d. **Final:**

Submit this report only if specifically requested by the appropriate CAA identified in Article 955. (**NOTE**: See Article 975 for final letter report format, content, and submission requirements.)

e. **Interim:**

If a final letter report is required but submission must be delayed because local inquiries/investigations are ongoing, an interim report must be submitted every 30 days until the final letter report is submitted. (**NOTE**: See Article 975 for interim report format, content, and submission requirements.)

955. CLOSING ACTION AUTHORITIES (CAAs) AND RESPONSIBILITIES

a. Identification of CAAs:

Command Preparing Report:	**CAA:**	
Coast Guard:	COGARD TISCOM ALEXANDRIA	
Marine Corps:	CMC WASHINGTON DC//CSB//	
Military Sealift:	COMSC WASHINGTON DC//N62M//	
Navy:	CINCLANTFLT NORFOLK VA//N6//	**OR**
Fleet/shore activities administratively subordinate to a FLTCINC	CINCUSNAVEUR LONDON UK//N6//	**OR**
	CINCPACFLT HONOLULU HI//N6//	
Navy shore activity not administra -tively subordinate to a FLTCINC or COMSC	DCMS WASHINGTON DC//20//	
Naval reserve force units and activities	COMNAVRESFOR NEW ORLEANS LA//01D//	

NOTE: If required by the CAA, the final letter report will be submitted within 30 days after the initial report or the last amplifying report. The final letter report will include a summary of the results of all inquiries and investigations, and it must identify corrective measures taken or planned to minimize the possibility of recurrence. (**NOTE:** If requested by a non -DON CA, corrective measures will be provided to that CA by separate message or be included in an amplifying report.)

b. CAA Responsibilities:

(1) As stated elsewhere in this chapter, the CAA determines the need for further reporting and has the authority

to request final letter reports for COMSEC incidents evaluated as "COMPROMISE" **or** "COMPROMISE CANNOT BE RULED OUT." Each CAA message or letter request for a final letter report must be addressed as follows:

From: CAA
ACTION: Violating Command

INFO: Administrative Chain of Command OR
Operational
Senior (as appropriate)
DCMS WASHINGTON DC//20//

Subject: REQUEST FOR FINAL LETTER REPORT

(2) CAAs must formally "close -out" only those cases for which a final letter report has been requested.

(a) After receiving the final letter report, the CAA will effect case closure by issuing a Closing Action Letter or Message to the violating command.

(b) The administrative Chain of Command or Operational Senior of the violating command and DCMS//20// must be included as copy to/information addressees.

(c) An example Closing Action Letter is provided in Figure 9 -3.

c. DCMS Responsibilities:

(1) Whenever a COMSEC incident is reported, DCMS as the DON CIMA, establishes an incident case file for the violating command. This case file facilitates tracking of all reports associated with the incident.

(2) DCMS is also responsible to "close -out" incident cases following submission of all required reports.

(a) Incident cases pending a final letter report will remain open until DCMS receives the CAA Closing Action Letter or Message.

(b) DCMS will close all other incident cases 30 days after receipt of the initial and/or amplifying report.

960. FORMAT AND CONTENT OF INITIAL AND AMPLIFYING REPORTS

a. General:

(1) Format and content requirements are outlined below. Each of the paragraphs indicated must be addressed in all initial reports.

(2) Where the reporting requirements of a paragraph are not applicable to the incident being reported, the corresponding paragraph in the report must reflect the notation "N/A" for not applicable.

(3) Where subsequent reports (e.g., amplifying) would merely duplicate information previously reported, the information need not be repeated. Instead, reference will be made to the previous report which contains the information.

b. Subject of Report: The subject of each report will be:

INITIAL REPORT OF COMSEC INCIDENT **OR**

AMPLIFYING REPORT OF COMSEC INCIDENT, as appropriate.

c. References: As applicable, the report must include references to:

(1) Identification of the paragraph number of the operating or maintenance instruction, or this manual in which the reported insecurity is listed.

(2) Previously forwarded reports relating to the incident (e.g., message date -time -group, letter serial number).

d. Body/Text of Report: The following information must be provided in the order presented here:

(1) **PARAGRAPH 1:** Identify the CMS account number of the violating command or activity. If the actual violator is a LH or User of the CMS account identified, state so here.

(2) **PARAGRAPH 2:** Identify the material involved as follows:

(a) Documents, hard-copy keying material, and electronic key converted from keytape:

Include the full short title and edition; accounting number; specific segments, tables, pages, if not a complete edition or document; the classification, and the CA of each short title listed.

(b) Field-generated key: List the short title, key designator, tag, or other identifier; circuit designator; type of crypto equipment used to secure the circuit; and type of key generator.

(c) Equipment (including CCI): Include the nomenclature or system designator; modification number(s) if applicable; serial number of AL 1 equipment (all other by quantity); and associated or host equipment. If the equipment was keyed, also identify the information previously identified for keying material.

(3) PARAGRAPH 3: Identify the personnel involved. Provide duty position and level of security clearance. For personnel incidents **only**, also provide name and rank/grade.

(4) PARAGRAPH 4: Describe the circumstances surrounding the incident. Give a chronological account of the events which led to the discovery of the incident and, when known, sufficient details to give a clear picture of how the incident occurred. If the reason for the incident is not known, describe the events that led to the discovery of the incident.

(5) **PARAGRAPH 5:** Provide command estimate of possibility of compromise with one of the following opinions:

(a) CO MPROMISE,

(b) COMPROMISE CANNOT BE RULED OUT, **OR**

(c) NO COMPROMISE.

NOTE: Refer to Article 980 for guidance on assessing compromise probability.

(6) **PARAGRAPH 6:** Provide the information requested below each of the following incidents that follow:

(a) CRYPTOGRAPHIC INCIDENTS:

(1) INCORRECT USE OF COMSEC KEYING MATERIAL **OR** USE OF AN UNAPPROVED OPERATING PROCEDURE:

--- Describe the communications activity (e.g., on-line/off-line, simplex/half-duplex/full-duplex, point-to-point/netted operations) and the operating mode of the COMSEC equipment (e.g., clock start, message indicator).

--- Estimate amount and type of traffic involved.

--- Estimate length of time the key was used.

(2) USE OF MALFUNCTIONING COMSEC EQUIPMENT:

--- Describe symptoms of the COMSEC equipment malfunction.

--- Estimate likelihood that the malfunction was deliberately indu ced. If so, also see Item (3) of this category.

(3) UNAUTHORIZED MODIFICATION OR MAINTENANCE OF COMSEC EQUIPMENT:

--- Describe the modification or device, installation, symptoms, host equipment involved, and protective technology, if applicable.

--- Estimate how long the item may have been in place.

--- Estimate the amount and type of traffic involved.

--- Identify the counterintelligence organiz ation notified (e.g., NIS for DON accounts), if applicable.

Include a point of contact and telephone number at the counter -intelligence organization.

(b) PERSONNEL INCIDENTS:

KNOWN OR SUSPECTED DEFECTION, ESPIONAGE, ATTEMPTED RECRUITMENT, UNAUTHORIZED ABSENCE, SABOTAGE, CAPTURE, HOSTILE COGNIZANT AGENCY ACTIVITY, OR TREASON:

--- Describe the individual's extent of knowledge of COMSEC and cryptoprinciples and protective technologies.

--- List the cryptosystems to which the individual had recent access and whether the access included keying material.

--- Identify the counterintelligence organization notified (e.g., NIS for DON accounts). Provide a point of contact and telephone number at the counterintelligence organization.

NOTE: Incidents related to unauthorized absence are to be reported only when there is missing material **or** reason to suspect espionage/defection.

(c) PHYSICAL INCIDENTS:

(1) UNAUTHORIZED ACCESS TO COMSEC MATERIAL:

--- Estimate how long unauthorized personnel had access to the material.

--- State whether espionage is suspected. If so, see items under personnel incidents above.

(2) LOSS OF COMSEC MATERIAL:

--- Describe the circumstances of last sighting; provide any available information concerning the cause of disappearance.

--- Describe the actions 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 waste and the possibility of loss by those methods.

(3) COMSEC MATERIAL DISCOVERED OUTSIDE OF REQUIRED COMSEC CONTROL OR ACCOUNTABILITY **OR** LOSS OF TPI :

--- Describe the action that caused accountability or physical control to be restored.

(c) PHYSICAL INCIDENTS : (continued)

--- Estimate likelihood of unauthorized access.

--- Estimate the length of time the material wa s unsecured.

(4) RECEIPT OF CLASSIFIED EQUIPMENT, CCI EQUIPMENT, OR KEYING MATERIAL MARKED OR DESIGNATED CRYPTO WITH A DAMAGE INNER WRAPPER :

--- Give a complete description of the damage.

--- If damage occurred in -transit, identify the method of shipment. Include the package number and point of origin.

--- If the damage occurred in storage, describe how the material was stored.

--- Estimate the likelihood of unauthorized access or viewing.

--- Ensure all packaging containers, wrappers, etc., are retained until disposition instructions are received.

(5) KNOWN OR SUSPECTED TAMPERING WITH COMSEC EQUIPMENT **OR** PENETRATION OF PROTECTIVE TECHNOLOGY :

--- Describe the evidence of tampering or penetration.

--- If the suspected tampering or penetration occurred in-transit, identify the method of shipment. Include the package number and point of origin.

--- If the suspected tampering or penetration occurred in storage, describe how the material was stored.

--- Identify the counterintelligence organization notified (e.g., NIS for DON accounts). Provide a point of

contact and telephone number at the counterintelligence organization.

--- Identify the date or serial number stamped on the protective techn ology, as applicable.

(6) UNAUTHORIZED PHOTOGRAPHY OR REPRODUCTION :

--- Identify the material or equipment that was reproduced or photographed.

--- Provide the reason for the reproduction and describe how the material was controlled.

--- Specify detail contained in the photographs of equipment internals.

--- State whether espionage is suspected. If so, also see items under the Personnel Incident Category on page 9 -16.

--- If the incident is evaluated as "COMPROMI SE" or "COMPROMISE CANNOT BE RULED OUT," forward a copy of each photograph or reproduction to NSA//V51A//. (R

(7) AIRCRAFT OR MISSILE CRASH :

--- Identify the location of the crash (including coordinates), and specify whether the crash occurred in friendly or hostile territory. If the aircraft/missile crashed at sea, also see Item (8) below.

--- State whether the aircraft/missile remained largely intact or if wreckage was scattered over a large area. Estimate the si ze of the area.

--- State whether the area was secured. If so, indicate how soon after the crash and by whom.

--- State whether recovery efforts for COMSEC material were made or are anticipated.

(8) MATERIAL LOST AT SEA :

--- Provide the coordinates (when available) or the approximate distance and direction from shore.

--- Estimate the depth of the water.

--- Estimate whether material was in weighted containers or was observed to sink.

--- Estimate the sea state, tidal tendency, and the most probable landfall.

--- State whether U.S. salvage efforts were made **or** are anticipated.

--- State whether foreign vessels were observed in the immediate area and their registry, if known.

--- Estimate the possibility of successful salvage operations by unfriendly nations.

(9) SPACE VEHICLE MISHAP :

--- Provide the launch area and time.

--- State whether the space vehicle was destroyed or lost in space.

--- State whether the keying material involved was unique to the operation or is common to other operations.

--- Estimate the probable impact point on the surface of the earth, if applicable. If the impact point was on land, also see Item (c) (7); if the impact point was at sea, see Item (c) (8).

(10) MISSING MOBILE UNIT (e.g., land vehicle, aircraft, or ship):

--- Identify the scheduled or probable route, probable or confirmed position, and date and time of last confirmed position (if available).

--- Estimate possibility of missing unit encountering hostile forces.

--- State whether recovery efforts for COMSEC material were made or are anticipated.

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

(8) PARAGRAPH 8: Indicate whether an SF 153 Relief from Accountability or Possession Report will be forwarded. If so, identify transaction number, if known.

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

965. PRECEDENCE AND TIMEFRAMES FOR SUBMITTING INITIAL REPORTS. Initial incident reports must be reported by message in accordance with the following precedence and timeframes:

a. Submit an **IMMEDIATE** precedence message within **24 hours** after discovery if the incident involves:

(1) Effective key.

(2) Key scheduled to become effective within 15 days.

(3) Incidents involving espionage, subversion, defection, theft, tampering, clandestine exploitation, sabotage, hostile cognizant agent activity, or unauthorized copying, photographing or reproduction.

NOTE: Following the submission of an IMMEDIATE precedence incident is available to rapidly respond to possible questions from

b. Submit a **PRIORITY** precedence message within **48 hours** after discovery if the incident involves:

(1) Future key scheduled to become effective in more than 15 days.

(2) Superseded key.

(3) Reserve on board (ROB) key.

(4) Contingency key.

c. Submit a **ROUTINE** precedence message within **72 hours** after discovery if the incident involves:

Any incident **not** covered above.

970. ADDRESSEES FOR COMSEC INCIDENT REPORTS

a. This article provides the **minimum** addressee requirements for submitting a COMSEC incident report. Additional addressees may be imposed at the discretion of the Chain(s) of Command of an account.

b. Where two-holder, point-to-point material is involved, the organization or unit that established the circuit will normally serve as controlling authority.

c. Address COMSEC incidents reports as indicated below based on the following categories:

(1) FIELD-GENERATED KEY (e.g., key generated by a KG-83, KGX-93):

ACTION: CA (See **NOTE** on next page for exceptions)

INFO: DIRNSA FT GEORGE G MEADE MD//V51A// (R
DCMS WASHINGTO N DC//20//
Closing Action Authority
Operational Chain of Command
Servicing A&A Team

(2) WHEN CONTROLLING AUTHORITY CAUSED THE INCIDENT:

ACTION: DCMS WASHINGTON DC//20//
DIRNSA FT GEORGE G MEADE MD//V51A// (R

INFO: COMNAVCOMTELCOM WASHINGTON

DC//N32/N3/N3X//
Closing Action Authority
Operational Chain of Command
Servicing A&A Team

(continued on next page)

(3) (a) NSA-PRODUCED KEY MARKED OR DESIGNATED CRYPTO (includes electronic key converted from tape key),

(b) CLASSIFIED COMSEC MATERIAL PRODUCED OR CONTROLLED BY NSA OTHER THAN KEYING MATERIAL ,

(c) CONTROLLED CRYPTOGRAPHIC ITEMS (CCI) :

ACTION: CA (See NOTE below for exceptions)

INFO: DIRNSA FT GEORGE G MEADE MD//V51A//
(NOTE: Omit when DIRNSA is the CA)
Closing Action Authority
Administrative Chain of Command
COMNAVCOMTELCOM WASHINGTON DC//N32/N3/N3X//
DCMS WASHINGTON DC//20// (**NOTE:** Omit when DCMS is the CA)
Servicing A&A Team

NOTE: 1. Address initial report for action to DCMS WASHINGTON DC//20// if:

A DON CA is the violator.

A PHYSICAL incident and there is more than one CA and they are all DON.

A loss of TPI involving SECRET and/or CONFIDENTIAL keying material marked or designated CRYPTO. (**NOTE:** Only those losses of TPI involving TOP SECRET key are reported to the CA or DIRNSA, as appropriate.)

2. Address initial report for action to DIRNSA FT GEORGE G MEADE MD//V51A// if:

A CRYPTOGRAPHIC or PERSONNEL incident.

A PHYSICAL incident involving known or suspected tampering of an EQUIPMENT or cryptosystem, sabotage, covert penetration, clandestine exploitation.

A PHYSICAL incident and there are multiple CAs and they are not all DON.

The CA cannot be determined.

(4) **CLASSIFIED COMSEC MATERIAL -RELATED PUBLICATIONS, MANUALS, OPERATING INSTRUCTIONS PRODUCED BY DEPARTMENTS AND AGENCIES OTHER THAN NSA AND DCMS :**

ACTION: CA or Promulgating Authority

INFO: DCMS WASHINGTON DC//20// (**NOTE:** Omit when DCMS is the CA)
DIRNSA FT GEORGE G MEADE MD//V51A//
(**NOTE:** Omit when DIRNSA is the CA)
Closing Action Authority
Administrative Chain of Command

(5) CLASSIFIED COMSEC MATERIAL -RELATED PUBLICATIONS AND MANUALS PRODUCED BY DCMS (e.g., CMSR, CMS 5A SUPP 1) :

Handle in accordance with OPNAVINST 5510.1 (series), Chapter 4, and request replacement (if desired) in accordance with Chapter 10 of this manual.

(6) UNCLASSIFIED COMSEC AND COMSEC -RELATED MATERIAL :

Report, and request replacement, in accordance with Chapter 10.

d. In accordance with OPNAVINST 5510.1 (series), the following commands must be included as information addressees in the distribution of initial reports of possible loss or compromise of **classified** material:

INFO: CNO WASHINGTON DC//N09N2//
COMNISCOM WASHINGTON DC
Nearest NIS Field Office (**NOTE:** See OPNAVINST 5510.1 (series) for a listing of NIS field offices.)

NOTE: Units afloat that do not have a Naval Investigative Service Resident Agent (NISRA) on board must include the NISRA nearest their homeport regardless of operating area. When the above addressees are included in the distribution of initial reports of actual or possible loss or compromise, the OPNAVINST 5510.1 (series) requirement for a preliminary inquiry is satisfied.

e. If an incident involves nuclear command and control COMSEC material other than JCS -positive control material, address the report for action to DIRNSA FT GEORGE G MEADE MD//V6//.

f. If an incident involves COMSEC material provided by the U.S. to allied governments, include DIRNSA FT GEORGE G MEADE MD//S11// as an information addressee.

g. If an incident involves actual or possible penetration of protective technologies, address the report for action to DIRNSA FT GEORGE G MEADE MD//Y264//.

975. FINAL LETTER AND INTERIM REPORT FORMAT, CONTENT, AND SUBMISSION REQUIREMENTS

a. Final Letter Report:

(1) The final letter report is the most comprehensive report of an incident. Final letter reports are required only when specifically requested by the CAA of the violating command.

(2) Final letter reports may be requested for keying and/or non-keying materials, as deemed appropriate by the CAA.

(3) CAAs may request final letter reports for incidents that have been evaluated by the CA of the material or other evaluating authority as, "COMPROMISE or COMPROMISE CANNOT BE RULED OUT."

(4) The final letter report must be submitted to the CAA via the administrative Chain of Command. The following report distribution requirements also apply, as applicable:

(a) Operating forces operationally subordinate to a FLTCINC but administratively subordinate to another FLTCINC will submit reports to the Administrative Senior with a copy to the Operational Senior.

(b) Shore commands not administratively subordinate to a FLTCINC, but which support a FLTCINC, will provide a copy to that FLTCINC.

(c) If DCMS is the CAA and the reporting command has imposed or is recommending disciplinary action, the final letter report must be forwarded via the reporting unit's next senior command with court martial jurisdiction over the incident to ensure proper legal review.

(d) Final letter reports must be submitted within 30 days of the initial report of the incident. CAAs will ensure that the final report is submitted within the prescribed timeframes.

(e) Final letter reports are used **only** within the DON. Final letter reports may **not** be sent to commands or units outside the DON (e.g., Army, Air Force, DIRNSA). (**NOTE:** If requested by a non-DON CA, corrective measures will be provided to that CA by separate message or be included in an amplifying report.)

(f) The final letter report format shown at the end of this chapter should be used whenever possible. The final letter report must include a comprehensive and complete report of the investigation conducted into the incident, and must state action taken by the command to prevent recurrence of the same type of incident.

b. Interim Report:

(1) If the final letter report cannot be completed and forwarded within 30 days of the submission of the initial report, an interim report must be submitted. The interim report must, at a minimum:

(a) Reference the initial report.

(b) Indicate the progress of the inquiry or investigation.

(c) Summarize any new development since the last report.

(d) Provide a brief statement explaining the reason(s) for the delay in submitting the final report.

(2) Submit the interim report(s) to the same addressees as for the final letter report.

980. ASSESSING COMPROMISE PROBABILITY

a. COMSEC incidents are evaluated using one of these terms:

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

(2) **COMPROMISE CANNOT 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.

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

b. Compromise probability assessment is often a subjective process, even for experienced evaluators who possess all pertinent facts concerning a COMSEC incident. To assist your command in assessing compromise probability, the following guidance is provided for the most commonly encountered or reported incidents:

(1) Lost keying material, including keying material believed to have been destroyed without documentation, and material that is temporarily out of control (believed lost but later recovered under circumstances where continuous secure handling cannot be assured or was found in an unauthorized location): Assess as COMPROMISE.

(2) Unauthorized access: If the person had the capability and opportunity to gain detailed knowledge of, or to alter information or material: Assess as COMPROMISE. If the person was under escort or under the observation of a person authorized access, or if physical controls were sufficient to prevent the person from obtaining detailed knowledge of information or material, or from altering it: Assess as NO COMPROMISE.

(3) Late destruction (not performed within required timeframe) of COMSEC material: If the material was properly

stored or safeguarded: Assess as NO COMPROMISE. If the storage or safeguarding procedures were questionable: Assess as COMPROMISE CANNOT BE RULED OUT.

(4) Unauthorized absence of personnel who have access to keying material: Assess as NO COMPROMISE, unless there is evidence of theft, loss of keying material, or defection.

NOTE: Whenever a person having access to keying material is reported as UA, all material he/she could have accessed **must** be inventoried. If there is evidence of theft or loss of keying material, or defection of personnel, the material must be considered COMPROMISED.

c. Also see NAG -16 (series) for guidance on assessing incidents involving field -generated electronic key.

985. REPORTING COMSEC INCIDENTS DURING TACTICAL DEPLOYMENTS AND DURING ACTUAL HOSTILITIES

a. During time -sensitive tactical deployments, abbreviated reports may be submitted for incidents involving keying material where espionage is not suspected.

b. Such reports must answer the questions: who, what, where, when, and how. This type of report must be submitted promptly to the addressees in Article 970 and must provide sufficient details to enable the evaluating authority to assess whether a compromise has occurred.

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

d. It is recognized that there will be times when immediate reporting to activities other than the controlling authority serves no purpose. When keying material that is scheduled for supersession within 48 hours is lost and espionage is not suspected, an incident report is not required.

INITIAL AND AMPLIFYING COMSEC INCIDENT REPORT FORMAT AND CONTENT CHECKLIST

Subject		_____
References		_____
Paragraph 1:	CMS account number	_____
Paragraph 2:	Material involved	_____
Paragraph 3:	Personnel involved	_____
Paragraph 4:	Circumstances of incident	_____
Paragraph 5:	Command compromise assessment	_____
Paragraph 6:	Additional information on incident required by:	_____

	Article 960 d. (6):
Incorrect use of COMSEC keying material or use of an unapproved operating procedure.	(a)(1)
Use of malfunctioning COMSEC equipment.	(a)(2)
Unauthorized modification or maintenance of COMSEC equipment.	(a)(3)
Known or suspected defection, espionage, attempted, recruitment, treason, sabotage, or capture.	(b)
Unauthorized access to COMSEC material.	(c)(1)
Loss of COMSEC material.	(c)(2)
COMSEC material discovered outside of required control or accountability.	(c)(3)
Loss of TPI.	(c)(3)
Receipt of classified equipment, CCI equipment, or keying material marked or designated CRYPTO with a damaged inner wrapper.	(c)(4)
Known or suspected tampering with COMSEC equipment or penetration of Protective Technology.	(c)(5)

FIGURE 9-1

INITIAL AND AMPLIFYING COMSEC INCIDENT REPORT FORMAT AND CONTENT CHECKLIST

Paragraph 6: Additional information on incident required by:

	Article 960 d. (6):
Unauthorized photography or reproduction.	(c)(6)
Aircraft or missile crash.	(c)(7)
Material lost at sea.	(c)(8)
Space vehicle mishap.	(c)(9)
Missing mobile unit.	(c)(10)

Paragraph 7: Whether investigation conducted. _____

Paragraph 8: Whether SF 153 Relief from Accountability or Possession Accounting Report will be submitted. _____

Paragraph 9: Point of contact and phone number. _____

FIGURE 9-1

EXAMPLE FINAL LETTER REPORT

NOTE: This example is classified for illustrative purposes only. The classification of an actual incident report must be determined by the command submitting the report based on the content of the report.

CONFIDENTIAL Closing Action Authority

From: USS ALWAYS AFLOAT (FF-00)
To: Commanding in Chief, U.S. Pacific Fleet
Via: (1) Commander, Cruiser-Destroyer Group One
(2) Commander, Naval Surfac Force Pacific

Subj: FINAL LETTER REPORT (CMS ACCOUNT NR xxxxxx) (U)

Ref: (a) CMS 1
(b) USS ALWAYS AFLOAT 251423Z MAY 93

If DCMS is the CAA, and the submitting commanding has imposed or is recommending disciplinary action, the Final Letter Report must be forwarded via the next senior command with court martial jurisdiction over the incident to ensure proper legal review. CAAs are identified in article 955a.

1. In accordance with reference (a), the following information is submitted with respect to the COMSEC incident reported by reference (b).

In paragraph 1, identify initial report and provide a synopsis of the incident.

a. Card 23 of AMSY 1234....

b. On 24 May, a daily inventory was taken of COMSEC material issued to radio central. Inventory results revealed on card (day 23) of AMSY 1234 was missing and presumed lost....

2. Upon completion of inventory, destruction of the superseded keying material was carried out in accordance with CMS 1, documented on CMS 25 forms, and verified by custodian and alternate. While extracting superseded keying material from the previous days, operator inadvertently removed Day 23 records which revealed that days 21 and 22 of AMSY 1234 were destroyed on 23 May. The destruction conducted on 23 May was performed hastily, and that haste led to the inaccuracy in accountability. On 24 May, the oncoming watch section discovered the card missing during the daily inventory of COMSEC material in radio central. A thorough search of radio central was conducted. The search accounts for the delay in submission of the initial report.

In paragraph 2, include a comprehensive presentation of all the facts involved, together with an analysis of all inquiries and investigations. The letter must contain the most complete information possible in order to permit full understanding of the nature and consequences of the occurrence.

3. The following measures have been taken to prevent recurrence.

In paragraph 3, identify recurrence: corrective measures taken to minimize the possibility of

a. Revised directives have been issued concerning handling and destruction of COMSEC material.

FIGURE 9-2

EXAMPLE FINAL LETTER REPORT (Cont'd)

b. CMS user training will be held twice a month once a quarter, emphasizing correct destruction procedures.

(C.O. SIGNATURE)

Copy to:
DCMS WASHINGTON DC

If a JAG Manual inventigation was vice done copies of the record of proceedings msut be forwarded to the CAA, COMNAVCOMTELCOM, and DCMS. Do not submit copies of the record of proceedings to the controlling authority of the material.

FIRST ENDORSEMENT ON...

From: Commander, Cruiser-Destroyer Group One
To: Commander in Chief, U.S. Pacific Fleet
Via: Commander, Naval Surface Force Pacific

ACTION BY VIA ADDRESSEES : Each endorsement MUST include opinions and comments on the incident, especially on the adequancy of corrective measures taken to minimize the possibility of recurrence. Endorsement MUST be completed within 30 days of receipt of the Final Letter Report. Requests for delaying endorsements beyond 30 days must be directed to the CAA, info the remaining endorsing commands.

SECOND ENDORESMENT on....

From: Commander, Naval Surface Force Pacific
To: Commander in Chief, U.S. Pacific Fleet

Copy to:
COMCRUDESGRU ONE
USS ALWAYS AFLOAT
DCMS WASHINGTON DC

From: Commander in Chief, U.S. Pacific Fleet
To: USS ALWAYS AFLOAT

ACTION BY CAA : When the CAA's review of the violation has been completed, a closing action letter must be prepared indicating administrative disposition and containing any instruction or comments which are considered appropriate. The initial report and the Final Letter Report must be referenced. The CAA letter must be addressed to the vilolating command, copy to DCMS.

Copy to:
DCMS WASHINGTON DC

FIGURE 9-2

EXAMPLE CLOSING ACTION LETTER

From: (CAA)
To: (Violating Command)

Subj: CLOSING ACTION LETTER

Ref: (a) (Final Letter Report)
(b) CMS 1
(c) (Initial/Amplifying incident report)

1. Originator takes reference (a) for action in accordance with reference (b).

2. Concur with reference (a) opinions, conclusions, and recommendations concerning reference (c) insecurity.

3. This case is closed.

4. Retain this letter and related reference in your CMS Correspondence file in
accordance with reference (b).

5. (CAA point of contact).

(Signature)

Copy to:
DCMS WASHINGTON DC (20)

FIGURE 9-3

CHAPTER 10 - PRACTICES DANGEROUS TO SECURITY (PDSs)

CHAPTER 10 - PRACTICES DANGEROUS TO SECURITY (PDSs)

1001. GENERAL

a. PDSs, while not reportable to the national level (NSA), are practices which have the potential to jeopardize the security of COMSEC material, **if** allowed to perpetuate.

b. All CMS accounts must conduct PDS familiarization training that will, at a minimum, include a review and discussion of this chapter. Document training locally in accordance with command directives.

1005. IDENTIFICATION OF PDSs

a. **The following is a list of NON -reportable PDSs:**

(1) Improperly completed accounting reports (i.e., unauthorized signatures, missing signatures or required accounting information, incomplete short title information).

(2) COMSEC keying material transferred with status markings still intact.

(3) COMSEC material not listed on account, local holder (LH), or user inventory documents.

(4) Issue of keying material, without authorization, to a LH or User more than 30 days before its effective period.

(5) Late destruction (includes key in a fill device) of COMSEC material (i.e., destruction not completed within the timeframes in this manual), except where a waiver has been granted.

NOTE: Superseded material received in an ROB shipment must be destroyed within 12 hours of opening the shipment. Annotate on the SF 153, "SUPERSEDED UPON RECEIPT." No additional reporting is required.

(6) Removing keying material from its protective packaging prior to issue for use, or removing the protective packaging without authorization, as long as the removal was documented and there was no reason to suspect espionage.

(7) Receipt of a package with a damaged outer wrapper, but an intact inner wrapper.

(8) Activation of the anti-tamper mechanism on, or unexplained zeroization of, COMSEC equipment, as long as no other indications of unauthorized access or penetration were present.

b. **The following PDSs must be reported OUTSIDE the command as indicated in Article 1010:**

(1) Premature or out-of-sequence use of keying material before its effective date, as long as the material was not reused.

NOTE: Premature use is defined as an on-the-air attempt to establish communications/transmit data. If material prematurely used is reused without consent ofthe CA, report as a CRYPTOGRAPHIC incident in accordance with Chapter 9.

(2) Inadvertent (i.e., early) destruction of COMSEC material, or destruction without authorization of the controlling authority (CA), as long as the destruction was properly documented. **(NOTE:** Whenever this occurs, annotate the destruction record of the material as follows: **"Material destruction was not authorized, but was properly destroyed and witnessed.")**

1010. REPORTING AND DOCUMENTATION REQUIREMENTS

a. PDS 1005 b. (1) **must** be reported to the CA of the material, information to DCMS//30//, so that implementation schedules can be adjusted.

b. PDS 1005 b. (2) **must** be reported outside the command in accordance with the following:

(1) Replacement material **NOT** required: Report inadvertent destruction to CA only.

(2) Replacement material required: Forward a message as follows:

ACTION: DCMS WASHINGTON DC//20/30//

INFO: Controlling Authority
CMIO
(other addressees as may be directed by the Chain of Command)
Servicing A&A Team

Subject: RESUPPLY DUE TO INADVERTENT DESTRUCTION

(1) CMS account number and HCI (e.g., 313233/TS).

(2) Short title, edition, accounting (serial or register) number, (as applicable).

(3) Specify date material needed (e.g., 930720).

(4) Specify DCS or other activity for delivery of material, or indicate OTC pickup from a CMIO.

NOTE: Unless advised otherwise by the CA, DCMS will automatically direct issue of replacement material.

c. Except for the PDSs cited in this article, all other PDSs are reportable only to the CO of the account. **(NOTE:** LH accounts will report inadvertent destructions to the CO of the CMS account.)

d. PDS documentation and report retention requirements (if any), for other than the two reportable PDSs identified in paragraph a. and b., shall be determined by the CO of the CMS account.

1015. REPORTING THE LOSS OR FINDING OF UNCLASSIFIED COMSEC MATERIAL

a. The loss or finding of the following is **not** considered a PDS or COMSEC incident:

(1) Unclassified COMSEC equipment and/or related devices not designated CCI.

(2) Unclassified COMSEC -related information such as publications, maintenance manuals, or operating instructions.

(3) Unclassified keying material not marked or designated CRYPTO.

b. The loss or finding of the items in paragraph a. must be reported to DCMS to effect replacement of a missing item or to obtain disposition instructions for a found item.

c. Submit a facsimile, letter, or message as follows:

ACTION: DCMS WASHINGTON DC//20/30//

INFO: CMIO

(other addressees as may be directed by the Chain of Command)

Subject: REPLACEMENT OF MISSING UNCLAS MATERIAL

OR

DISPO INSTS FOR FOUND UNCLAS MATERIAL

(1) CMS account number.

(2) Identity of material (i.e., short title, edition, accounting (serial or register) number, CA or promulgating authority).

(3) If applicable, date material needed.

(4) If applicable, specify DCS or other activity for delivery of material, or indicate OTC pickup from a CMIO.

CHAPTER 11 - MANAGEMENT OF ELECTRONIC KEY

1101. Introduction

1102. Purpose

1105. Scope

1110. Limitations

1115. Responsibilities

1120. Definitions

1125. Crypto-Equipment Capabilities

1130. Types of Key

1135. TPI Requirements (G eneral)

1140. Safeguarding Requirements for Keyed Crypto-Equipment

1145. Certifying and Handling Key Variable Generators (KVGs)

1150. Sources of Electronic Key

a. KEK
b. TEK
c. Start-up KEK
d. KW-46 Key
e. General guidance

1153. Generation of Key by Field Sites

a. KG-83 and KGX-93/93A KVGs
b. KY-57/58/67 and KYV-5/KY-99/99A

1155. Classification of Electronic Key

a. Field-generated electronic key
b. Electronic key converted from tape key
c. In COMSEC emergencies

1160. Allocation of Electronic Key

a. OTAR KEK
b. OTAR/OTAT TEK
c. Start-up KEK

CHAPTER 11 - MANAGEMENT OF ELECTRONIC KEY

1165. Distribution of 128-Bit Electronic Key

- a. KEK
- b. TEK
- c. Distribution via KW-46
- d. SCI/SI Key restrictions
- e. Tactical OTAT of TEK via STU-III

1166. Timing of OTAT Key Distribution

1170. Notification of Impending Key Transfer (OTAT)

- a. Transmitting station must notify
- b. Notification must include

1175. Tagging/Identi fication of OTAT Key

1176. Handling of KEK and TEK

- a. KEK
- b. TEK

1177. Electronic Key Storage

1178. Cryptoperiods

- a. KEK
- b. TEK

1179. Key Tape Ordering

1180. Physical Transfer of Electronic Key in FD

1181. Inventory Requirement for Electronic Key

1182. Accountability and Reporting Requirements

1183. Reporting of COMSEC Incidents for Electronic Key

1184. NAG 16 ( )

CHAPTER 11 - MANAGEMENT OF ELECTRONIC KEY

1101. INTRODUCTION

a. The Nation al and DON policy is to implement an electronic key system and virtually eliminate the use of paper-based keying materials by the year 2000.

b. The procedures described in this chapter and in NAG 16 (series) [1], Field Generation and Over-the-Air Distribution of COMSEC Key in Support of Tactical Operations and Exercises, describe a joint standard for conducting over-the-air distribution (OTAD). These techniques and methods are consistent with allied procedures contained in ACP 132A and will effectively support combined as well as joint operations.

c. When implemented, OTAD procedures will improve operational key management flexibility, improve security through greater user of locally generated key, and reduce reliance on logistically unsupportable paper-based systems. Use of OTAD will also increase personnel awareness in proper handling and safeguarding techniques for electronic key.

1102. PURPOSE

a. This chapter describes the policies and procedures for generating, handling, safeguarding, and distributing 128-bit electronic COMSEC key.

b. NAG 16 ( ) is prescribed as the standard user's manual for planning and conducting electronic key generation, over-the-air rekeying (OTAR), and over-the-air key transfer (OTAT).

c. Procedures detailed in this chapter:

(1) **Supplement** those contained in NAG 16 ( ).
(2) Address requirements that are DON unique
(3) Provide a basis for standardization within DON

d. Some of the basic doctrine for OTAR/OTAT in NAG 16 ( ) is repeated in this chapter for ease of use.

e. See Article 1184 for information not addressed in this chapter, yet contained in NAG 16 ( ).

NOTE: 1. Because NAG 16 ( ) is not accountable in the CMCS, copies may be reproduced locally as required. Account commands that were not issued copies of NAG 16 ( ) may request them from CMIO Norfolk.

2. Foreign release of NAG 16 ( ) must be preapproved by DIRNSA (Code I1).

---

[1] NAG 16 ( ) is held by tactical forces of all U.S. services and its combined equivalent, ACP-132, is held by tactical military forces of Australia, Canada, New Zealand, the United Kingdom, and by some U.S. tactical forces.

1105. SCOPE

a. Military commanders at all levels are authorized to direct field generation and distribution of electronic COMSEC key to support operations or exercises and are encouraged to do so.

b. While procedures herein primarily address DON requirements, utilization of electronic key procedures are applicable to U.S. joint and intra-service operations and exercises, and can also be used with allied units [2] that have OTAR/OTAT capable crypto-equipment.

c. Procedures in this chapter apply to fleet broadcasts, point-to-point circuits, and multi-station nets.

d. Electroni c key may be converted from key tape or generated by certified KG-83/KGX-93/93A key variable generators, by KY-57/58/67 (VINSON/BANCROFT), and KYV-5/KY-99/99A (ANDVT) equipment.

e. Electronic key may be distributed electronically, via OTAR or OTAT, or physically in a fill device (FD).

1110. LIMITATIONS

a. Detailed policies/procedures for Joint Tactical Communications System (TRI-TAC) and Mobile Subscriber Equipment (MSE) secure communication systems are not contained in this chapter. See NAG 16 ( ) for more detailed guidance.

b. Procedures herein address routine operational practices, but exceptions are authorized under **COMSEC emergencies** (i.e., the only viable alternative being plain text communications) as determined by the CO/on-scene commander. Implementation of other than prescribed procedures must be in support of an urgent and unforeseen operational requirement and not become routine practices.

1115. RESPONSIBILITIES

a. Field generation and electronic distribution are the **preferred** means for providing electronic key to DON tactical forces. Commanders responsible for key provisioning to such forces should endeavor to produce locally the tactical 128-bit key they require and distribute it via over-the-air key distribution (OTAD). Specifically, commands authorized a KG-83 are expected to employ locally generated key to support limited scale operations. KG-83

[2] Allied units that use OTAR-capable, "S" nomenclatured (special purpose), COMSEC equipment may receive traffic encryption key (TEK) via OTAR, but are not authorized to serve as net control stations (NCSs) for combined nets and circuits that distribute electronic key via OTAR. NAG-22A, Over-the-Air Rekeying of Combined Tactical Nets, was produced to explain OTAR and OTAT to these allies. U.S. tactical forces and allied tactical forces that hold ACP-132 do not need NAG-22A.

holders ashore will use the KG to generate TEK for point-to-point circuits as well as KEK where the electronic KEK can be physically transferred in a FD to authorized recipients. Additional guidance follows:

(1) Carrier battle group and amphibious ready group commanders should establish OTAR-capable, intra-force and embarked amphibious force nets/circuits using a start-up KEK, should generate intra-force OTAR TEKs with the KG-83s allocated to their flagships, and should OTAR the generated key to ships in company.

(2) Marine forces should generate OTAR TEK for their KY-57/58/67 and KYV-5/KY-99/99A secured nets/circuits at the NCSs and distribute them via OTAR and should generate other 128-bit tactical key in TRI-TAC key variable generators (KVGs), if available.

(3) The commander who directs field generation of electronic key becomes its controlling authority (CA); see Annex C of this manual. Electronic key converted from tape key remains under the purview of the designated CA.

(4) Submarine commanders and any commander who regularly holds material in excess of normal reserve on board (ROB) should employ OTAD to reduce holdings of material which historically have been used sparsely.

b. Custodian personnel are not required to supervise or witness the generation, relay, transfer, receipt, or destruction of locally generated electronic key. These actions may be executed by any personnel who are fully qualified and authorized access to COMSEC keying material.

c. Custodian personnel are responsible for overseeing the implementation of and compliance with this chapter (e.g., aperiodic review of local logs, adherence to TPI requirements).

1120. DEFINITIONS

Definitions and commonly used abbreviations/acronyms in this chapter are contained in Annexes A and B, respectively.

1125. CRYPTO-EQUIPMENT CAPABILITIES

U.S. crypto-equipment capable of field generating electronic key and/or distributing it over the air are identified in paragraph II. of NAG 16 ( ).

1130. TYPES OF KEY

a. The principal types of key covered in this chapter are as follows:

(1) **Key Encryption Key (KEK)**: Key that encrypts or decrypts other key for transmission or storage.

(2) **Start-Up KEK**: Key encryption key held in common by a group of potential communicating entities and used to establish ad hoc tactical nets.

(3) **Traffic Encryption Key (TEK)**: Key used to encrypt plain text or to superencrypt previously encrypted text and/or to decrypt cipher text.

1135. TWO-PERSON INTEGRITY (TPI) REQUIREMENTS (GENERAL)

a. TPI requirements are addressed in detail in article 510. Requirements stated in this chapter are repeated for emphasis and are applicable for key and equipments associated with OTAR/OTAT operations.

b. Classified key marked CRYPTO and its electronic equivalents in common fill devices (FDs) must be provided TPI handling and storage. Authorized exceptions to this rule are outlined in article 510.

NOTE: TPI requirements for classified key stored in Data Transfer Devices (DTDs or AN/CYZ-10s) are in Annex AD.

c. Unclassified key in tape or electronic form does **not** require TPI handling and storage.

d. Classified electronic key requires TPI handling whenever it is generated, distributed electronically or received via OTAT. There are no TPI requirements for recipients of key received via OTAR under conditions where **no** FD is required at the receiving terminal.

e. Non-DON recipients (e.g., Army, Air Force) are only required to adhere to national doctrine that mandates TPI for Top Secret key only. This applies even when non-DON personnel routinely receive key from a DON account as users of the account.

f. When KG-83s are not being used to transfer generated key into a FD, their "Dutch doors" must be double-locked with TPI-approved combination locks.

1140. SAFEGUARDING REQUIREMENTS FOR KEYED CRYPTO-EQUIPMENT

a. TPI safeguards are not required for keyed COMSEC equipment located in spaces that are **continuously** occupied by appropriately cleared persons who are in sight of each other **and** the keyed equipment.

b. Keyed COMSEC equipment used to terminate part-time nets/circuits may be left in unattended spaces, provided the equipment has been rekeyed by OTAR or updating with the next future TEK immediately before terminal close-down. Reasonable security measures must be taken (e.g., locking a door and controlling access) to prevent theft, tampering, or unauthorized operation of a keyed terminal when unattended.

c. Keyed COMSEC equipment used to terminate full-time nets/circuits may be left in unattended spaces only if such spaces meet DON criteria for open storage of information classified at the level of the TEK used.

1145. CERTIFYING AND HANDLING KEY VARIABLE GENERATORS (KVGs)

a. KG-83s have been distributed to afloat and shore commands in accordance with the KG-83 Master Plan. KG-83 KVGs are used by Navy and Coast Guard to generate OTAR TEK for use with KG-84A/84C secured nets and circuits. KGX-93/93A KVGs are used by the Marine Corps to generate key for TRITAC switches.

b. KG-83 and KGX-93/93A KVGs used to produce operational key must be certified prior to initial use, annually thereafter, following maintenance, and whenever security control is lost (e.g., KVG is found outside of proper storage and unattended). This certification process provides the necessary assurance that the equipment is functioning according to design specifications.

NOTE: There are no certification requirements for KY-57/58/67 and KYV-5/KY-99/99A equipments.

c. Certification must be performed by two qualified technicians using NSA-prescribed routines and KT-83 test equipment.

d. Certified KG-83 and KGX-93/93A KVGs are authorized to generate 128-bit keys for any purpose, up to the classification level to which they have been certified.

e. Marine Corps elements are responsible for certifying their own KGX-93/93As. Marine Corps KGX-93/93As are certified and repaired by Electronic Maintenance Companies (ELMACO), Communications Battalions (CommBn's), Communications Squadrons (CommSq's), and Communications Companies (CommCo's).

f. NISEWEST CRF San Diego is the primary location for recertification of KG-83s. NISEEAST Charleston has been tasked to manage the certification of KG-83 devices. This includes maintenance of a database containing all KG-83 devices within DON, serial numbers, holder, and recertification dates. The database program automatically identifies those KG-83 devices requiring recertification.

(1) Due to a two-month certification pipeline, all KG-83s will enter the certification process two months prior to expiration. NISEWEST CRF San Diego will notify the holder by message that a

replacement KG-83 has been forwarded. Upon receipt of the new KG-83, the holder will remove the old KG-83 from service and pack and ship the old KG-83.

(2) If a KG-83's certification is scheduled to expire within **30 days** and a replacement KG-83 has not been received, the using command must notify NISEEAST CHARLESTON SC//422// by message (Info DCMS WASHINGTON DC//30//, the using command's ISIC and operational commander).

(3) If a KVG's certificate expires while its user is awaiting delivery of a certified replacement, the user may continue to use the affected KVG and should **not** report the situation as a COMSEC incident.

g. If a KG-83 or KGX-93/93A fails, the using command must request a certified replacement by message from NISEEAST CHARLESTON SC//433// (INFO DCMS WASHINGTON DC//30//, the using command's ISIC and operational commander). While waiting for the replacement, the

certification, command that performed certification, and name and rank of certifying technicians. Such tags are to be prepared locally at certification sites and are to be tied securely to one of the KVG handles.

j. Users of KG-83s and KGX-93s must examine applied tamper detection labels when a new KVG is received and at least monthly thereafter. Detection of a damaged label invalidates a KVG's certification and must be reported as a COMSEC incident (see Chapter 9). The affected KVG must then be recertified.

k. Certified KG-83s must be stored as Top Secret COMSEC material under no-lone zone (NLZ) at repair sites. When installed in operational communications environments, certified KG-83s need not be afforded TPI or NLZ protection, **provided** their "dutch doors" are double-locked with TPI-approved combination locks.

l. Certified KGX-93/93As must be stored as Secret COMSEC material at recertification sites.

m. Certified KG-83s mu st be shipped under TPI safeguards when certified to the Top Secret level. Certified KGX-93/93As must be shipped using any of the methods approved in article 530 for Secret COMSEC equipment.

n. When installed in TRI-TAC switches, certified KGX-93s, to which tamper detection labels have been applied, must be locked into place (by two authorized persons using the two-person access lock). Providing this is accomplished, certified KGX-93s need not be removed when their locked shelters are left unmanned.

o. Decertified KG-83s and KGX-93/93As, including those being returned for certification, must be handled as Confidential COMSEC material and may be shipped via U.S. registered mail (provided it does not pass through a foreign postal system or foreign inspection), Defense Courier Service (DCS), Cleared Commercial Carriers using Protective Security Service, or U.S. military contract service (e.g., AMC, LOGAIR, QUICKTRANS).

NOTE: **l**. Registered mail sent to FPO AE/AP addresses does NOT pass out of U.S. cont rol.
2. In **COMSEC emergencies**, a KVG with an expired certification may be used, pending its recertification or replacement with a certified equipment.
3. In **COMSEC emergencies**, a KVG that is certified Secret may be used to generate Top Secret key until a Top Secret certified replacement is obtained.

1150. SOURCES OF ELECTRONIC KEY

NOTE: The types and sources of key associated with OTAD are fully detailed in NAG 16 ( ) (paragraphs III.C. and III.D.). **Abbreviated** information on these keys is provided here for ease of use.

a. KEK:

(1) Normally produced in tape form and held at using locations. However, when all users are located close enough to the producer/source it may be field-generated and delivered in FDs.

(2) **In COMSEC emergencies**, any uncompromised, classified key that is held in common by affected commands and that is not used for any other purpose may serve temporarily as KG-84A/84C/KIV-7, KY-57/58/67, or KYV-5/KY-99/99A KEK, until properly classified KEK can be provided.

b. TEK:

(1) Generated electronically by an authorized KVG [3], converted from tape key, or held in tape form. KVGs may generate 128-bit TEK for any of the COMSEC systems listed in NAG 16C (Annex K).

(2) **In COMSEC emergencies**, any uncompromised, classified key that is controlled by the using NCS and that is not used for any other purpose may be used as OTAR TEK.

NOTE: **Except in COMSEC emergencies**, TEK generated by KY-57/58/67 and KYV-5/KY-99/99A equipments is restricted to use i n their respective cryptosystem families.

c. Start-up KEK:

(1) Normally produced in tape form or converted from tape to electronic form and delivered physically in FDs.

(2) **In COMSEC emergencies**, individual segments of start-up KEK may be distributed via OTAT.

NOTE: KEK, TEK, and start-up KEK are used in cryptonets operating with KG-84A/84C/KIV-7, KY-57/58/67, and KYV-5/KY-99/99A equipments only.

d. KW-46 Key: The KW-46 uses three types of key:

(1) Broadcast Area Variable (BAV) p roduced in tape form and delivered to users encrypted in that unit's unique variable.

(2) Unique Variable (UV) produced in tape form, and

(3) Community Variable (CV) produced in tape form, but may also be generated by certified KG-83/KGX-93/93A KVGs or converted from tape key and distributed in a FD or electronically via OTAR/OTAT.

[3]To the maximum extent possible, military commanders should field-generate the TEK needed to support their operations and exercises.

NOTE: See NAG 16 ( ) for additional information on the use of KW-46 keys and for KW-46 OTAR/OTAT communications procedures.

e. General Guidance:

(1) Carrie r battle groups and amphibious ready group commanders should establish OTAR-capable, intra-force nets and circuits using a start-up KEK, should generate intra-force OTAR TEKs with the KG-83 KVGs allocated to their flagships, and should distribute the keys to ships in company via OTAR. Carrier battle groups and amphibious ready groups are encouraged to requisition their own start-up KEKs, so that a start-up KEK having the smallest distribution may be used to create tactical nets/circuits.

(2) Marine f orces should generate OTAR TEK for their KY-57/58/67 and KYV-5/KY-99/99A secured nets and circuits at the respective NCSs and distribute them via OTAR.

(3) Navy and Coast Guard broadcast stations should generate and distribute via OTAT the key required by ships and afloat commanders they support.

1153. GENERATION OF KEY BY FIELD SITES

a. KG-83 and KGX-93/93A KVGs:

KG-83/KGX-93/93A KVGs are authorized to generate 128-bit key up to the classification to which they have been certified. Key generated by these equipments are authorized for use with any crypto-equipment that uses 128-bit key.

NOTE: SCI/SI cleared personnel may use KG-83/KGX-93/KGX-93A equipment located in GENSER spaces to generate 128-bit key for use on SCI/SI protected circuits.

b. KY-57/58/67 and KYV-5/KY-99/99A:

Except in COMSEC emergencies, key generated by these equipments is restricted to use in their respective families.

1155. CLASSIFICATION OF ELECTRONIC KEY

a. Field-generated electronic ke y, while not physically marked with a classification, must be handled/stored based on the highest classification of information to be protected or the TEK being passed.

b. Electronic key converted from tape key must be handled/stored at the same level of classification as the tape key from which it was converted.

c. **In COMSEC emergencies**, classified electronic key may be used to secure information classified one level higher than its classification.

1160. ALLOCATION OF ELECTRONIC KEY

a. OTAR KEK must be allocated as follows:

(1) Point-to-Point (PTP) circuits :

(a) Each PTP circuit that is secured by KG-84A/84C/KIV-7s, KY-57/58/67s, or KYV-5/KY-99/99A must use a unique short title of KEK.

NOTE: For security reasons, it is important that multiple KG-84A/84C/KIV-7 secured PTP circuits that terminate in the same NCS be keyed with separate OTAR TEK and not with a common OTAT TEK, as would be appropriate for multiple-station radio nets in tactical environments.

(b) For parallel KG-84A/KG-84C/KIV-7 secured circuits terminating in the same space at both terminals, the same short title may be used with the parallel circuits, but separate tape segments must be used for each circuit.

NOTE: **In COMSEC emergencies**, common KEK may be used for all PTP circuits controlled by a NCS, until separate, two-copy KEK can be provided for use with each out station (OS).

(2) Multi-station nets :

(a) The NCS for each multi-station net that distributes TEK via OTAR must specify whether OTAR will be accomplished sequentially (i.e., one OS at a time) or simultaneously for all net OSs (see NAG 16 ( ), paragraph III.D.1.d (2)).

(b) If a NCS uses the sequential method, each OS must have a unique KEK short title.

(c) All net OSs must hold a common KEK (or start-up KEK) when the simultaneous method is used.

NOTE: Creation of a net with start-up KEK automatically provides common KEK for all net OSs and mandates simultaneous OTAR.

b. OTAR/OTAT TEK must be allocated as follows: A unique segment of OTAR TEK or a unique, field-generated OTAR TEK must be used on each KY-57/58/67, KG-84A/84C/KIV-7, or KYV-5/KY-99/99A secured net/circuit.

c. Start-up KEK must be allocated as follows:

(1) Each edition of start-up KEK is produced in the "VA" format (62 segments, daily cryptoperiod) and is effective for two months.

(2) Segment use is based on a predictable day/date relationship (e.g., segment 5B may be used only on the fifth day of the second month that an edition is effective). Segments 1A - 31A are used during the first month, and segments 1B - 31B are for use during the second month.

(3) Each segment of start-up KEK is effective for only one radio day. During that day, any tactical commander who holds a KYX-15 or DTD (AN/CYZ-10) may use the effective segment to activate any number of OTAR-capable nets or circuits (see NAG 16 ( ), paragraph III.D.2).

NOTE: Use of start-up KEK is limited to tactical forces requiring the establish ment of temporary circuits/nets in support of temporary operations/exercises.

1165. DISTRIBUTION OF 128-BIT ELECTRONIC KEY

a. KEK:

(1) Distribute physically in tape form or by FD after electronic conversion/generation.

(2) In shore establishment environments where the same COMSEC account distributes OTAR KEK to all members of a complex of KG-84A/84C/KIV-7 secured PTP circuits (e.g., an NAS supporting aircraft squadrons), it is not necessary to procure tape OTAR KEK to link each OS with the NCS. A unique OTAR KEK for each link can be extracted from a certified KVG and delivered quarterly to each OS in a FD or a unique segment of the NCS's OTAR TEK can be allocated to serve as the KEK for each link and be delivered quarterly to each OS.

(3) **In COMSEC emergencies**, KEK (and individual segments of start-up KEK) may be passed via OTAT, until physical distribution in tape form can be arranged.

b. TEK:

(1) To maximum extent possible, distribute TEK electronically, via OTAR or OTAT.

(2) If KEK of proper classification is used, any 128-bit tactical TEK may be distributed via OTAT, using STU-III/DTD

terminals [4], KW-46 secured broadcasts, KG-84A/84C/KIV-7, KY-57/58/67, or KYV-5/KY-99/99A secured nets/circuits.

c. Distribution via KW-46 :

(1) The GENSER broadcast channels are limited to distribution of key protecting GENSER circuits only.

(2) OPINTEL broadcast channels are authorized to distribute key for both GENSER and SCI/SI circuits.

(3) The four Naval Computer an d Telecommunications Area Master Stations (NCTAMS) are authorized to generate and distribute by OTAR and/or OTAT the KW-46 CVs that are required to support the U.S. surface broadcast channels they originate. However, worldwide back-up CVs (one each for GENSER and SCI/SI) will be retained in contingency status for use in the event of some unforeseen requirement.

(4) KW-46 CVs that are field-generated or converted from tape may be distributed on KW-46 secured broadcasts via OTAT, for extraction via a FD, or via OTAR, for use in the receiving KWR-46.

NOTE: Extraction of key from a KW-46 receive terminal is restricted to authorized recipients only. All broadcast subscribers must zeroize their KW-46 extraction registers immediately after completion of key transfer. Key that is received via OTAT in the UVRQ/Rekey register that is not intended for use by a command may be zeroized by a single operator.

d. SCI/SI Key restrictions :

(1) Except when specifically authorized by the CA, OTAT of SCI/SI TEK is restricted to transmission via circuitry protected by SCI/SI key.

(2) Procedures established by the CA for passing SCI/SI key in other than SCI/SI protected circuits, must be strictly followed to preclude the possible compromise of SCI/SI information.

e. Tactical OTAT of TEK via STU-III :

(1) When connected to a DTD (AN/CYZ-10), a STU-III terminal may be used to transfer unencrypted (red) tactical TEK for tactical use, and their associated key tags, to a distant STU-III so configured.

(2) Each of the communicating STU-IIIs must meet the following requirements:

[4]Any tactical TEK may be transmitted via OTAT using the secure mode of STU-III secured telephone circuits having DTDs (AN/CYZ-10s) attached.

(a) Be in the secure data mode.

(b) A NSA-approved connector cable and cable adaptor must be used between the STU-III and the DTD.

(c) The DTD must use NSA's standard STU-III compatible fill application software package.

(d) Have a unit-specific department/agency/organization (DAO) description on the second line of their non-scrolling STU-III display.

NOTE: An example of a unit- specific DAO description is "USS SARATOGA." To prepare for OTAT, tactical units that do not have unit-specific DAO descriptions should order new STU-III key associated with such descriptions. For more information on DAO descriptions, see CMS 6 and EKMS 702.01.

(3) See NAG 16 ( ), Annex J, for the procedures for transferring key and tag from one DTD to another via STU-III.

1166. TIMING OF OTAT KEY DISTRIBUTION

TEK may be distributed via OTAT at any time during its effective cryptoperiod, and the cryptoperiod immediately preceding that in which it is to become effective (e.g., weekly cryptoperiod KG-84C TEK that is generated by a field station may be passed anytime during the week preceding its intended implementation).

1170. NOTIFICATION OF IMPENDING KEY TRANSFER (OTAT)

a. A transmitting station must notify all recipients of key to be passed via OTAT prior to the actual transmission of key.

b. The notification must include the following:

(1) Time key will be transmitted.

(2) Identity of the circuit on which key will be sent.

(3) Destination instructions for recipients (i.e., device/circuit for which the key is intended).

(4) Identification of the key to be transmitted, to include short title, classification, effective period, and CA.

1175. TAGGING/IDENTIFICATION OF OTAT KEY

a. Electronically generated key for transmission via OTAT must be tagged/marked to allow immediate recognition of the key. A tag or designator will be assigned to key by the generating station.

(1) Tagging field-generated key: The generator of the key will tag the key by using three fields of information. Each field and its description will be as follows:

(a) **Field 1**: A two-digit number which represents the number of electronic keys produced by the generating station. It is assigned in a one-up sequence and will restart daily at 0001Z.

(b) **Field 2**: This field will identify the CA.

(c) **Field 3**: The Julian date the key was generated.

EXAMPLE: "01C7FLT365" - 01 represents the first key generated. C7FLT represents COMSEVENTHFLT, and 365 represents the Julian date the key was generated.

NOTE: Key tags should not exceed ten characters (i.e., letters/numbers).

(2) Tagging key converted from tape key: Electronic key converted from tape key will be tagged by using four fields of information. Each field and its description will be as follows:

(a) **Field 1**: Identification of key as either Allied (A) or U.S. (U).

(b) **Field 2**: Identification of the four or five digits of the short title.

(c) **Field 3**: One or two-letter identification of the edition.

(d) **Field 4**: One or two-digit identification of the segment number.

EXAMPLE: "U1019BC07" - U for USKAT, short title 1019, edition BC, segment 07.

b. Additional identification requirements:

(1) In addition to the tagging of electronic key, the transmitting station must notify all recipients in advance of transmitting the key and provide the information contained in Article 1170.

(2) All commands that handle electronic key will, as required, maintain local accounting records and clearly label the identity of key contained in FDs. Article 1182 contains procedures for maintaining local accounting records.

1176. HANDLING OF KEK AND TEK

a. KEK: Each tape segment and/or its electronic equivalent, held in a FD, may be used only on its designated circuit and must be destroyed no later than 12 hours after the end of its cryptoperiod.

b. TEK: Each tape segment and/or its electronic equivalent, held in a FD, must be destroyed/zeroized after completing an operation successfully in accordance with the following:

(1) Relay stations must zeroize their FDs immediately after confirming successful relay of OTAT key.

(2) End users of key, except for NCSs and NCTAMs in KG-84A/84C/KIV-7, KY-57/58/67, or KYV-5/KY-99/99A nets, should normally destroy their TEK held in FDs immediately after establishing communications, but are authorized to retain TEK held in FDs throughout the effective period of the key (if required for operational purposes). The TEK must be destroyed no later than 12 hours after the end of its cryptoperiod.

(3) NCSs and NCTAMs for KG-84A/84C/KIV-7, KY-57/58/67, or KYV-5/KY-99/99A nets are authorized to retain OTAT TEK in tape form (when electronic key is converted from tape key) and its electronic equivalent in a FD, throughout its effective cryptoperiod. The key, all forms, must be destroyed no later than 12 hours after the end of its cryptoperiod.

1177. ELECTRONIC KEY STORAGE

a. Generally, key may be stored as follows:

(1) Recipients of physical transfers of key loaded in a FD (passed from one person to another) are authorized to store key in their FDs until operationally required.

(2) Recipients, less relay stations, of key passed via OTAT are authorized to store key in their FDs until operationally required.

(3) Relay stations must zeroize their fill devices within 12 hours after confirming that a successful OTAT relay has taken place.

(4) NCSs and NCTAMs for KG-84A/84C/KIV-7, KY-57/58/67, or KYV-5/KY-99/99A/KY-75 nets are authorized to retain TEK (tape and/or electronic) throughout its effective cryptoperiod.

b. TEK and KEK may be used/stored in the same FD.

c. Classified key stored in a common FD must be afforded TPI handling/storage as required by Article 1135. The key will be zeroized no later than 12 hours after the end of its cryptoperiod.

1178. CRYPTOPERIODS FOR KEK AND TEK

a. KEK: The maximum cryptoperiod for each segment of KG-84A/84C/KIV-7, KY-57/58/67, or KYV-5/KY-99/99A KEK (except for start-up KEK) is three months. CAs may extend cryptoperiods for up to seven days without report. Longer extensions must have prior NSA approval or be reported as a COMSEC incident.

NOTE: Each segment of KG-84A/84C/KIV-7 KEK has a maximum cryptoperiod of three months, even if it is drawn from an edition that is then routinely superseded. Unless the affected KEK has been compromised, continue d use of such key throughout its 3-month cryptoperiod is authorized.

b. TEK: One month is the normal cryptoperiod for KG-84A/84C, KY-57/58/67, and KYV-5/KY-99/99A TEK used on tactical nets/circuits that operate continuously while they are active (i.e., that do not close down for specified periods).

NOTE: See NAG 16 ( ) for additional information on TEK cryptoperiods.

1179. KEY TAPE ORDERING

For guidance in ordering key tape (e.g., TEK for OTAR, KEK, and start-up KEK) , see NAG 16 ( ) (Annex B).

1180. PHYSICAL TRANSFER OF ELECTRONIC KEY IN A FD

a. The physical transfer of electronic key refers to the exchange of key in a FD from one person to another for use at another location at the same command or a different command. Transfer of key in this manner is authorized provided that the recipients are properly cleared and authorized to hold the key.

NOTE: The transfer of key to a non-authorized holder must be approved by the CA of the key.

b. Recipients of electronic key in a FD mus t acknowledge receipt of the key by signing a local custody document.

(1) Thereafter, each location holding the key must properly safeguard and continuously account for the loaded FD, by serial number, until the key is zeroized, overwritten, or otherwise destroyed.

(2) Minimum accounting information for the key must include the short title or designator of the key, date of generation/loading, number of copies made, date of transfer, identity of generator and recipient, classification, CA, and effective period of the key.

1181. INVENTORY REQUIREMENT FOR ELECTRONIC KEY

a. There is no inventory requirement for electronic key. Accountability and control must be maintained by the application of TPI for FDs and crypto-equipment which permits generation or extraction of key, and local accounting records.

b. Inventory of tape key is, however, required in accordance with the procedures in Chapter 7 of this manual.

1182. ACCOUNTABILITY AND REPORTING REQUIREMENTS

a. There is no requirement to report field generation of electronic key to DCMS.

b. Commands converting tape key to electronic form are not required to report distribution of this key to an authorized holder.

c. Distribution of key to an unauthorized holder must be authorized by the CA of the key. CAs must ensure that DCMS is notified of key distributed to other than an authorized holder. This action is necessary to ensure that all holders are notified in the event that emergency supersession of a key is required.

d. Except f or recipients of key received via OTAR, all commands that generate, transmit, relay, or receive electronic key are required to maintain local accounting records.

NOTE: There are no accounting requirements for recipients of key received via OTAR.

(1) **Key generation**: Commands that generate electronic key for OTAR/OTAT must retain local accounting records for a minimum of 60 days following the date of the last entry on the key generation log. Retention of local records applies to both field-generated key and key converted from tape key.

(2) **Key receipt/relay**: Commands relaying or receiving electronic key, except for recipients of OTAR key, must retain local accounting records until the key has been superseded.

NOTE: Commands converting tape key to electronic form for transmission via OTAR/OTAT must account for the tape key in accordance with its assigned AL code.

e. Copies of local accounting records for a generating station (OTAR/OTAT) and relaying/receiving stations (OTAT) are included in Annexes Q and R, respectively. Commands will fill in appropriate columns of the accounting records based on the action taken.

f. Recordkeeping/accounting requirements matrix :

OTAT		OTAR	
FLD GEN KEY	TAPE KEY	FLD GEN KEY	T

Commands must refer to NAG 16 ( ) for detailed information on the following:

a. Specific OTAR/OTAT co mmunications procedures (e.g., KW-46)

b. Allied OTAR doctrine

c. Use of ICP Generic Key as OTAR/OTAT KEK

d. Distributing key via DSN/AUTODIN, STU-III, TRI-TAC, and MSE

e. Unsuccessful OTAR situations

f. Late joiners to nets

g. Key tape ordering guidance

h. List of all 128-bit crypto-equipment

i. Procedures for transferring key and tag from one DTD (AN/CYZ-10) to another via STU-III.

ANNEX A

GLOSSARY

Access: The opportunity and capability to obtain knowledge of COMSEC material, or to use, copy, remove, or tamper with it. (NOTE: A person does not have access merely by being in a place where COMSEC material is kept, as long as security measures (e.g., physical, technical, or procedural) prevents them from having an opportunity to obtain knowledge of, or alter, information or material.)

Accounting legend (AL) code: A numeric code used in the COMSEC Material Control System (CMCS) to indicate the minimum accounting controls required for an item of accountable COMSEC material.

Accounting number: A number assigned to an individual item of COMSEC material to simplify its handling and accounting. (**NOTE**: Also referred to as register or serial number.)

Advice and Assistance (A&A) Training Team: Worldwide network of CMS subject matter experts who provide training and assistance to personnel with COMSEC responsibilities.

AL 1: AL 1 COMSEC material is continuously accountable by accounting (register/serial) number from production to destruction.

AL 2: AL 2 COMSEC material is continuously accountable by quantity from production to destruction.

D)
AL 4: AL 4 COMSEC material is locally accountable by quantity after initial receipt.

Alternate CMS Custodian(s): Individual(s) designated to assist the CMS Custodian in the performance of his/her duties and to perform Custodian duties during the temporary absence of the CMS Custodian. (**NOTE**: Alternate Custodians share equally with the CMS Custodian for the proper management of a CMS account.)

Amendment: A correction or change to a COMSEC publication.

ANNEX A

GLOSSARY

AMSG-293: NATO cryptographic instructions.

AMSG-600 (series): NATO Communications Security Information Memoranda. (NOTE: This publication, published semi-annually, provides status information for NATO COMSEC material.)

Assembly: A group of parts, elements, subassemblies, or circuits that are removable items of COMSEC equipment.

Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's eligibility to receive specific categories of information.

Authenticator: Means used to confirm the identity or eligibility of a station, originator, or individual.

Auto-manual system: Programmable, hand-held device used to perform encoding and decoding functions.

Automated information system (AIS): Any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data and includes computer hardware, firmware, and software. (NOTE: Included are computers, word processing systems, networks, or other electronic information handling systems, and associated equipment.

Automated Navy COMSEC Reporting System (ANCRS): Software program which permits CMS account custodians to maintain account records and generate CMS reports using a personal computer (PC).

Automatic remote rekeying (AK): Procedure to rekey a distant (A crypto-equipment electronically without specific actions by the receiving terminal operator.

Benign: Condition of cryptographic data such that it cannot be compromised by human access to the data. (NOTE: The term benign may be used to modify a variety of COMSEC-related terms (e.g., key, data, storage, fill, and key distribution techniques.)

ANNEX A

GLOSSARY

Binding: Process of associating a specific communications terminal with a specific cryptographic key or associating two related elements of information.

BLACK: Designation applied to telecommunications and automated information systems, and to associated areas, circuits, components, and equipment, in which only unclassified signals are processed. (NOTE: Encrypted signals are unclassified.)

Black bulk facility: A telecommunications facility that employs crypto-equipment to protect multichannel trunks passing encrypted or unclassified information.

BLACK key: Encrypted key.

Broadcast Area Variable (key) (BAV): This key is used in (A conjunction with two other keys, the Community Key (CV) and Unique Key (UV), for KW-46 secured broadcasts. Navy uses four separate BAVs for its broadcasts covering the Western
Pacific/Indian Ocean, Eastern Pacific, Atlantic and Mediterranean areas.

Bulk encryption: Simultaneous encryption of all channels of a multichannel telecommunications trunk.

Call sign cipher: Cryptosystems used to encipher/decipher call signs, address groups, and address indicating groups.

Canister: Type of protective package used to contain and dispense key in punched or printed tape form.

Central Facility (CF): Composite of NSA's Ft. Meade and Finksburg key facilities that provides centralized key management services for all forms of key. (NOTE: The CF is the NSA portion of EKMS. The CF will provide unique keys to DCMS/CMIO for distribution to DON CMS accounts.)

Central Office of Record (COR): A central office which keeps records of all accountable COMSEC material held by elements subject to its oversight. (NOTE: DCMS is the COR for the Navy, Marine Corps, Coast Guard, and Military Sealift Command CMS accounts, and as such, establishes/closes accounts, reconciles inventories, and responds to queries concerning account management. DCMS also maintains accountability and oversight for STU-III terminals.)

ANNEX A
GLOSSARY

Chief of Naval Operations (CNO): CNO (N652), Head, Navy Information Security (INFOSEC) Branch, has overall authority for Naval Telecommunications to include COMSEC policy. CNO is the COMSEC resource sponsor for the DON.

CINCLANTFLT/CINCPACFLT/CINUSNAVEURINST C2282.1 (series): Basic Shipboard Allowance of COMSEC Material. (NOTE: This instruction provides basic CMS account requirements for Atlantic/Pacific surface and subsurface units by hull type and ocean area.)

CJCSI 3260.1: Joint Policies and Procedures Governing Positive (A Control Material and Devices, dated 31 July 1995

Closing Action Authority (CAA): Administrative senior or other designated command that reviews details of incidents or insecurities reported by their subordinate commands.

CMS 1: CMS Policy and Procedures Manual.

CMS 2: CMS Advice and Assistance (A&A) Training Team Procedures.

CMS 3A: CMS Inspection Manual.

CMS 5A: CMS Cryptographic Equipment Information/Guidance Manual.

CMS 6: STU-III Policy and Procedures Manual.

CMS 17: Used to record COMSEC material issued on local custody.

CMS 25: Single-copy segmented COMSEC keying material destruction report.

CMS 25B: Bi-monthly single-copy segmented C OMSEC keying material destruction report.

CMS 25MC: Multiple-copy segmented COMSEC keying material destruction report.

CMS account: An administrative entity, identified by a six-digit account number, responsible for maintaining accountability, custody and control of COMSEC material. (NOTE: A CMS account may also hold STU-III COMSEC material.)

ANNEX A

GLOSSARY

CMS Clerk: An individual assigned to assist custodian personnel in the execution of certain administrative duties associated with the management of a CMS account. (NOTE: Appointment of a CMS Clerk is at the discretion of the Commanding Officer.)

CMS Custodian: Individual responsible for all actions associated with the receipt, handling, issue, safeguarding, accounting, and disposition of COMSEC material assigned to a command's CMS account.

CMS Form 1: Locally prepared form used to authorize appropriately cleared personnel to receipt for and courier COMSEC material between their command and a CMIO.

CMS User: Individual responsible for the proper security, control, accountability, and disposition of the COMSEC material placed in his/her charge. (NOTE: A CMS User may or may not have signed for COMSEC material.)

CMS Witness: Individual who assists custodian or user personnel in the proper execution of tasks related to the handling and safeguarding of COMSEC material (e.g., receipt, destruction, inventory, adherence to TPI handling requirements).

Code: System of communications in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length. (NOTE: Codes may or may not provide security. Common use includes: (a) converting information into a form suitable for communications or encryption, (b) reducing the length of time required to transmit information, (c) describing the instructions which control the operation of a computer, and (d) converting plain text to meaningless combinations of letters or numbers and vice versa.

Code book: Book or other document containing plain text and code equivalents in a systematic arrangement, or a technique of machine encryption using a word substitution technique.

Cold start: Procedure for initially keying crypto-equipment.

ANNEX A
GLOSSARY

COMDTINST M5500.11 (series): Coast Guard Security Manual. (NOTE: Provides regulations and guidance for Department of Transportation and Coast Guard units/personnel for classifying and safeguarding classified information and the protection of Coast Guard assets and personnel.)

Command authority: Individual responsible for the appointment of user representatives for a department, agency, or organizations and assignment of their key ordering privileges.

Commandant, Marine Corps (CMC): CMC (CSB) is the Marine Corps focal point for requirements and administration of Marine Corps CMS accounts. CMC is resource sponsor and works in coordination with CNO, COMNAVCOMTELCOM, and DCMS, in establishing, promulgating and overseeing Marine Corps CMS account management matters unique to the Marine Corps.

Commander, U.S. Coast Guard Telecommunications Information Systems Command (COGARD TISCOM): COGARD TISCOM (OPS4) exercises overall authority for all CG telecommunications issues, including COMSEC matters. OPS4 promulgates CG COMSEC policy and exercises service wide management of CG CMS accounts.

Commander, Naval Computer and Telecommunications Command (CNCTC): Implements the DON CMS program.

Commanding Officer (CO): Individual ultimately responsible for the proper administration of his/her command's CMS account and compliance with established CMS policy and procedures. (NOTE: An OIC has the same responsibilities as a CO.)

Communications Security (COMSEC): Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government concerning national security, and to ensure the authenticity of such telecommunications. (NOTE: COMSEC includes cryptosecurity, emission security, transmission security, and physical security of COMSEC material and COMSEC information.)

Community Variable (key) (CV): This key is used in conjunction (A with two other keys, the Broadcast Area Variable (BAV) and Unique Key (UV), for KW-46 for secured broadcasts. Separate tape CVs are used for Navy surface ship general service (GENSER) and submarine GENSER fleet broadcasts, the U.S. Navy Special Intelligence (SI) broadcasts, the U.S. Coast Guard broadcasts, and the NATO broadcasts. CVs may also be generated by certified KG-83/KGX-93/93A key variable generators and distributed electronically via OTAR or OTAT.

ANNEX A

GLOSSARY

Compromise: Disclosure of information or data to unauthorized person(s), or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

Computer security (COMPUSEC): Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer.

COMSEC aid: COMSEC material, other than an equipment or device, that assists in securing telecommunications and which is required in the production, operation, or maintenance of COMSEC systems and their components. (NOTE: COMSEC keying material, callsign/frequency systems, and supporting documentation, such as operating and maintenance manuals, are examples of COMSEC aids.)

COMSEC Automated Reporting System (CARS): System which uses a PC and a STU-III for transferring CMS reports to or from DCMS and accessing selected areas in the database at DCMS.

COMSEC emergency: Operational situation, as perceived by the responsible Commanding Officer/on-scene commander, in which the alternative to strict compliance with procedural restrictions affecting use of a COMSEC equipment would be plain text communications.

COMSEC equipment: Equipment designed to provide security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor and, subsequently, by reconverting such information to its original form for authorized recipients; also, equipment designed specifically to aid in, or as an essential element of, the conversion process. (NOTE: COMSEC equipment includes crypto, crypto-ancillary, crypto-production, and authentication equipment.)

COMSEC facility: Space employed primarily for the purpose of generating, storing, repairing, or using COMSEC material.

ANNEX A

GLOSSARY

COMSEC incident: Any uninvestigated or unevaluated occurrence that has the potential to jeopardize the security of COMSEC material or the secure transmission of classified or sensitive government information; OR any investigated or evaluated occurrence that has been determined as not jeopardizing the security of COMSEC material or the secure transmission of classified or sensitive government information. (NOTE: COMSEC incidents and insecurities are categorized as cryptographic, personnel, or physical.)

COMSEC Incident Monitoring Activity (CIMA): The office within a department or agency that keeps a record of COMSEC incidents and insecurities caused by elements of that department or agency, and ensures that all actions required of those elements are completed. (NOTE: DCMS is the CIMA for the DON.)

COMSEC insecurity: A COMSEC incident that has been investigated, evaluated, and determined to have jeopardized the security of COMSEC material or the secure transmission of classified or sensitive government information.

COMSEC material: Items designed to secure or authenticate telecommunications. (NOTE: COMSEC material includes, but is not limited to, key, equipment, devices, documents, firmware or software that embodies or describes cryptographic logic and other items that perform COMSEC functions.)

COMSEC Material Control System (CMCS): A logistics and accounting system through which COMSEC material is distributed, controlled, and safeguarded. (NOTE: The CMCS consists of all COMSEC CORs, cryptologistic depots, and CMS accounts.)

COMSEC Material Status Report (CMSR): Primary source of status information (NOTE: There are two forms; Master CMSR (MCMSR) and Customized CMSR (C2CMSR) which are identified further in this glossary.)

COMSUBLANT/PACNOTE C2280 (series): Basic COMSEC material allowance for submarine force.

Contingency key: Key held for use under specific operational conditions or in support of specific contingency plans. (NOTE: The CMSR will reflect this material as when directed (WHENDI).)

ANNEX A

GLOSSARY

Controlled cryptographic item (CCI): A secure telecommunications or information handling equipment, or associated cryptographic component, that is unclassified but governed by a special set of control requirements. (NOTE: Such items are marked "CONTROLLED CRYPTOGRAPHIC ITEM" or, where space is limited, "CCI".)

Controlling authority (CA): Designated official responsible for directing the operation of a circuit/cryptonet and for managing the operational use and control of keying material assigned to a circuit/cryptonet. (NOTE: The CA for field -generated electronic key is the Commander who directed generation of the key. Electronic key converted from tape key remains under the purview of the designated CA.)

CRYPTO: A marking or designator identifying COMSEC keying material used to secure or authenticate telecommunications carrying classified or sensitive U.S. government or U.S. government -derived information. (NOTE: When written in all upper case letters, CRYPTO has the meaning stated above. When written in lower case as a prefix, crypto and crypt are abbreviations for cryptographic. The caveat CRYPTO is applied only to key used on-the-air.)

Crypto-ancillary equipment: Equipment designed specifically to facilitate efficient or reliable operation of crypto -equipment, but that does not perform cryptographic functions.

Crypto-equipment: Equipment that embodies a cryptographic logic.

Cryptographic: Pertaining to, or connected with, cryptography.

Cryptographic incident: Any uninvestigated or unevaluated equipment malfunction, or operator or custodian error that has the potential to jeopardize the cryptosecurity of a machine, auto -manual, or manual cryptosystem OR any investigated or evaluated occurrence that has been determined as not jeopardizing the cryptosecurity of a machine, auto-manual, or manual cryptosystem.

Cryptographic insecurity: A crypto incident that has been investigated or evaluated and determined to have jeopardized the cryptosecurity of a machine, auto -manual, or manual cryptosystem.

ANNEX A

GLOSSARY

Cryptographic component: The hardware or firmware embodiment of the cryptographic logic in a secure telecommunications or automated information processing system. (NOTE: A cryptographic component may be a modular assembly, a printed wiring assembly (PWA), a microcircuit, or a combination of these items.)

Cryptography: Principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.

Crypto-ignition key (CIK): Device or electronic key used to unlock the secured mode of crypto -equipment.

Cryptonet: Three or more elements which use, in common, a short title of keying material.

Cryptoperiod: Time span during which each key setting (i.e., key segment or key card) remains in effect.

Cryptosecurity: Components of communications security that results from the provision of technically sound cryptosystems and their proper use.

Cryptosystem: Associated COMSEC items interacting to provide a single means of encryption or decryption.

Customized COMSEC Material Status Report (C2MSR): Lists only those keys and pubs our database records indicate are charged to your account as of the date of the report.

Data transfer device (DTD): A common fill device used to store and distribute electronic key. (NOTE: The DTD will be used to extract key from a LMD and then load the key directly into a cryptographic device.)

DCS Manual 5200.1 (series): Details administrative and operational procedures for the Defense Courier Service (DCS).

ANNEX A

GLOSSARY

Defense Courier Service (DCS): A joint command of the DOD. The DCS provides the principal means for the secure and rapid transportation of DOD and other qualified material requiring controlled handling by courier authorized customers. (NOTE: Majority of CMS accounts will receive their COMSEC keying material via the DCS.)

Director, Communications Security Material System (DCMS): Administers DON CMS program and functions as Central Office of Record (COR) for Navy, Marine Corps, Coast Guard and Military Sealift command CMS accounts.

Electrical transaction report (ETR): Formatted data fields used to report CMS transactions (e.g., receipt, transfer). (NOTE: ETRs may be forwarded via CARS or via message.)

Electronic key: Encrypted or unencrypted key in electronic form that is stored on magnetic media or in electronic memory, transferred by electronic circuitry, or loaded into COMSEC equipment.

Electronic Key Management System (EKMS): Interoperable collection of systems being developed by services and agencies of the U.S. Government to automate the planning, ordering, generating, distributing, storing, filling, using, and destroying electronic key and management of other types of COMSEC material. (NOTE: The Navy Key Distribution System (NKDS) is a part of EKMS.)

Electronically generated key: Key produced only in non -physical form. (NOTE: Electronically generated key stored magnetically (e.g., on a floppy disk) is not considered hard copy key.)

Element: Removable item of COMSEC equipment, assembly, or subassembly which normally consists of a single piece or group of replaceable parts.

Embedded cryptography: Cryptography which is engineered into an equipment or system the basic function of which is not cryptographic. (NOTE: Components comprising the cryptographic module are inside the equipment or system and share host device power and housing. The cryptographic function may be dispersed or identifiable as a separate module within the host.)

ANNEX A

GLOSSARY

Emergency modification of holdings: An unforeseen and urgent operational requirement, as determined by the Commanding Officer, which requires the immediate transfer of COMSEC material.

End-item accounting: Accounting for all of the accountable components of a COMSEC equipment by a single short title.

Evaluating authority: The official responsible for evaluating a reported COMSEC incident for possibility of compromise. (NOTE: In the case of COMSEC incidents involving keying material, the evaluating authority may or may not be the material's controlling authority.)

Exercise key: Key intended for protection of on -the-air transmissions associated with field training or exercises.

Extractable keying material: Keying material designed to permit physical extraction and removal of individual segments.

Extraction resistance: The capability of a crypto -equipment to resist efforts to extract loaded cryptovariables or key.

Fill device (FD): Any one of a family of devices developed to read in,

ANNEX A

GLOSSARY

Highest classification indicator (HCI): Used to determine the highest classification of COMSEC material that an account may hold. (NOTE: The HCI is determined by comparing the clearance level of assigned custodian personnel and then selecting the highest clearance they all have in common.)

Immediate Superior in Command (ISIC): Command responsible for the administrative oversight of all CMS matters for their subordinate commands.

Inter-service transfer: Transfer of COMSEC material between a DON CMS account and a CMS account of another service, agency, department, nation, or commercial contractor.

Intra-service transfer: Transfer of COMSEC material between two DON CMS accounts.

Intrusion detection system (IDS): A system designed to detect and signal the entry of unauthorized persons into a protected area (e.g., security alarms, sensor systems, video systems).

Inventory: 1. The physical verification or sighting of the presence of each item of accountable COMSEC material. 2. A listing of each item of accountable COMSEC material charged to a CMS account or maintained on local custody (i.e., material held by LH Custodian or Users).

Irregularly superseded keying material: Keying material that is superseded based on use and not on a pre -determined supersession date.

KAM: Cryptographic Operational Maintenance Manual or maintenance manual for a cryptosystem.

KAO: Cryptographic Operational Operating Manual or operating instructions for a cryptosystem.

ANNEX A
GLOSSARY

Key: Information (usually a sequence of random binary digits) used initially to set up and periodically change the operations performed in crypto -equipment for the purpose of en/decrypting electronic signals, for determining electronic counter -countermeasures patterns (e.g., frequency hopping or spread spectrum), or for producing other key. (NOTE: "Key" has replaced the terms "variable," "key(ing) variable," and "cryptovariable.")

Key encryption key (KEK): Key that encrypts or decrypts other key for transmission or storage.

Key list: Printed series of key settings for a specific cryptonet. (NOTE: Key lists may be produced in list, pad, or printed tape format.)

Key processor (KP): Cryptographic component in EKMS designed to provide for the local generation of keying material, encryption and decryption of key, key load into fill devices, and message signature functions. (NOTE: The KP will allow DCMS/CMIO to send electronic key to a CMS account. The KP will verify that the key is for a particular user and encrypt the key in an account's unique key for storage on the LMD.)

Key tape: Punched or magnetic tape containing key. (NOTE: Printed key in tape form is referred to as a key list.)

Key Variable Generator (KVG): A modular, rack mountable unit (A which, upon demand, generates 128-bit variables to key distribution centers, fill devices, or other equipment. It can be operated as a stand-alone device or in a rack in conjunction with other compatible equipment. In either case, the KVG generates variables and transfers them to the front or rear panel interface. KG-83 KVGs are used by the Navy and Coast Guard to generate OTAR TEK for use with KG-84A/84C secured nets and circuits. KGX-93/93A KVGs are used by the Marine Corps to generate key for TRITAC switches.

Keying material: A type of COMSEC item in physical or non -physical form which supplies either encoding means for manual and auto -manual cryptosystems or key for machine cryptosystems.

Key updating: Irreversible cryptographic process for modifying key automatically or manually.

Letter of Agreement (LOA): Defines requirements and responsibilities in those instances where a CMS account provides COMSEC material to a command that has a CO different from that of the CMS account.

Letter of Appointment (LOA): Used by COs to formally designate the assignment of custodian personnel and CMS Clerks.

ANNEX A

GLOSSARY

Limited maintenance: COMSEC maintenance restricted to fault isolation, removal, and replacement of plug -in assemblies.

Local custody: The acceptance of responsibility for the proper handling, safeguarding, accounting, and disposition of COMSEC material issued by custodian personnel or a user.

Local Holder account: Local Holder (LH) accounts are sub -accounts of a CMS account. (NOTE: A LH account has no account number and will normally receive its COMSEC material directly from a CMS account instead of from another source (e.g., a CMIO).)

Local Holder Alternate Custodian(s): Individual(s) designated to assist the LH Custodian in the performance of his/her duties and to perform custodian duties during the temporary absence of the LH Custodian. (NOTE: LH Alternate Custodians share equally with the LH Custodian for the proper management of a LH account.)

Local Holder Custodian: The LH Custodian is the individual responsible for managing COMSEC material issued by a CMS account to a LH account.

Local Management Device (LMD): Component (i.e., a personal computer (PC)) in EKMS/NKDS which provides automated services for the management of key and other COMSEC material, and an interface by which additional functionality may be incorporated to enhance its local capabilities. (NOTE: The LMD in NKDS will be a PC dedicated to CMS functions. Electronic key will be transmitted from DCMS/CMIO into the LMD for storage until required for use.)

Long title: Descriptive title of a COMSEC item.

Maintenance key: Key, not marked CRYPTO, which is intended only for off-the-air, in-shop use.

Manual cryptosystem: Cryptosystem in which the cryptographic processes are performed manually without the use of crypto -equipment or auto -manual devices.

ANNEX A

GLOSSARY

Manual remote rekeying (MK): Procedure by which a distant crypto-equipment is rekeyed electronically, with specific actions required by the receiving terminal.

Master COMSEC Material Status Report (MCMSR): Lists effective and supersession dates and other material information for all of the keys and publications that comprise the Navy's inventory.

Memorandum of Appointment (MOA): See Letter of Appointment.

Minimize: A condition imposed on users of DOD telecommunications networks where normal message and/or telephone traffic is drastically reduced so that messages connected with an actual or simulated emergency will not be delayed.

Mobile COMSEC facility: COMSEC facility that can be readily moved from one location to another (e.g., a van).

Mobile User: For COMSEC purposes, a term encompassing Marine Tactical, Naval Special Warfare (SPECWAR), Naval Construction Battalion, Mobile Inshore Undersea Warfare Surveillance, Explosive Ordnance Disposal (EOD) units, and all aircraft. (R (NOTE: Units identified above are considered mobile users when operating in a tactical/field environment at a temporary site away from their permanent operating base/area.)

Modification: Any NSA -approved mechanical change to the electrical, mechanical, or software characteristics of a COMSEC equipment, assembly, or device. (NOTE: Classes of modifications are: mandatory, optional/special mission, and repair action.)

NACSI 4009: National COMSEC Instruction - Protected Distribution Systems. (NOTE: Provides guidance concerning use of wirelines or fiber optics for the electrical or optical transmission of unencrypted classified information.)

NAG-16 (series): Field Production and Distribution of Electronic Key in Support of Short -Notice Operations. (NOTE: Annex C contains compromise assessment guidance for evaluating COMSEC incidents involving field -generated electronic key.)

ANNEX A

GLOSSARY

National COMSEC Incident & Reporting Evaluation System (NCIRES): System established by the National Security Agency (NSA) for evaluating incidents involving COMSEC material.

National Security Agency (NSA): Executive agent for developing and implementing national policy for COMSEC material. Produces and develops most COMSEC material used to secure the transmission of classified or sensitive unclassified information.

Navy Key Distribution System (NKDS): System designed to generate, protect, receive, distribute, transfer, and manage COMSEC material throughout the DON. (NOTE: NKDS is composed of the mainframe computers to be located at DCMS/CMIOs, and Local Management Devices (LMDs), Key Processors (KPs), and Data Transfer Devices (DTDs) which will be fielded to all CMS accounts.)

Net control station (NCS): Terminal in a secure telecommunications net responsible for distributing key in electronic form to the members of the net.

No-lone zone: An area, room, or space to which no one person may have unaccompanied access and which, when occupied, must be occupied by two or more appropriately cleared individuals who remain within sight of each other.

Non-extractable keying material: Keying material designed to remain intact (i.e., in its original physical form) throughout its entire effective period.

Operational key: Key, marked CRYPTO, intended for on -the-air protectio n of operational information or for the production or secure electrical transmission of key streams.

OPNAVINST 2221.3 (series): Communications Security (COMSEC) Equipment Maintenance and Training. (NOTE: This instruction provides training requirements for COMSEC equipment installation, maintenance, and repair.)

OPNAVINST 2221.5 (series): Release of COMSEC Material to U.S. Industrial Firms Under Contract to U.S. Navy. (NOTE: This instruction provides policy and procedures for authorizing release of COMSEC material to industrial firms under contract to USN.)

ANNEX A
GLOSSARY

OPNAVINST 5040.7 (series): Naval Command Inspection Program. (NOTE: This instruction assigns responsibility and prescribes procedures for the preparation, conduct, reporting, and follow -up of inspections.)

OPNAVINST 5510.1 (series): DON Information and Personnel Security Program Regulation. (NOTE: This instruction provides all DON activities and personnel with regulations and guidance for classifying and safeguarding classified information and for personnel security.)

OPNAVINST 5510.93 (series): Navy Implementation of National Policy on Control of Compromising Emanations. (NOTE: Promulgates within the DON, the policy and procedures for the implementation of the national policy on the control of compromising emanations.)

OPNAVINST 5530.14 (series): DON Physical Security and Loss Prevention Manual. (NOTE: This instruction provides standards for physical security and loss prevention measures to safeguard personnel, property, and material at Navy and Marine Corps shore installations and activities.)

Over-the-air key distribution (OTAD): Providing electronic key via over-the-air rekeying (OTAR), over -the-air key transfer (OTAT), or cooperative key generation.

Over-the-air key transfer (OTAT): Electronically distributing key without changing traffic encryption key (TEK) used on the secured communications path over which the transfer is accomplished.

Over-the-air rekeying (OTAR): Changing traffic encryption key (TEK) or transmission security key (TSK) in remote crypto -equipment by sending new key directly to the remote crypto -equipment over the communications path it secures.

Pagecheck: Verification that all pages of a publication or technical manual are present.

Personnel incident: An unevaluated or uninvestigated incident regarding the capture, attempted recruitment, or known or suspected control by a hostile intelligence entity, or unauthorized absence or defection of an individual having knowledge of or access to COMSEC information or material, that has the potential to jeopardize COMSEC information or material; OR any investigated or evaluated occurrence that has been determined as not jeopardizing COMSEC information or material.

ANNEX A
GLOSSARY

Personnel insecurity: A personnel incident that has been investigated or evaluated and determined to have jeopardized COMSEC information or material.

Physical incident: An unevaluated or uninvestigated incident regarding any loss of control, theft, capture, recovery by salvage, tampering, unauthorized viewing, access, or photographing that has the potential to jeopardize COMSEC material; OR any investigated or evaluated occurrence that has been determined as not jeopardizing COMSEC material.

Physical insecurity: A physical incident that has been evaluated or investigated and determined to have jeopardized COMSEC material.

Physical security: Physical measures designed to safeguard COMSEC material or information from being accessed or intercepted by unauthorized persons.

Positive control material and devices: A generic term referring to Joint Staff positive control material and devices which includes Sealed Authentication System (SAS), Permissive Action Link (PAL), Coded Switch System (CSS), Positive Enable System (PES), and Nuclear Certified Computer Data (NCCD). (NOTE: DCMS's role for positive control material is limited to accounting functions only.)

Protective packaging: Packaging techniques for COMSEC material which discourage penetration, reveal that a penetration has occurred or was attempted, or inhibit viewing or copying of keying material prior to the time it is exposed for use.

Protective technologies: Special tamper -evident features and materials employed for the purpose of detecting tampering and deterring attempts to compromise, modify, penetrate, extract, or substitute information processing equipment and keying material. (NOTE: Protective technologies include, but are not limited to, key tape canisters, end -opening key card packages, holographic bags, seals, screw head coating, and logo tape.)

Public key cryptography: Type of cryptography in which the encryption process is publicly available and unprotected, but in which a part of the decryption key is protected so that only a party with knowledge of both parts of the decryption process can decrypt the cipher text. (NOTE: Commonly called non -secret encryption in professional cryptologic circles. FIREFLY is an application of public key cryptography.)

ANNEX A
GLOSSARY

RED: Designation applied to telecommunications and automated information systems, plus associated areas, circuits, components, and equipment which, when classified plain text signals are being processed therein, require protection during electrical transmission.

RED key: Unencrypted key.

Regularly superseded keying material: Keying material that is superseded on a regular, pre -determined date for each edition of material regardless of whether or not the material has been used.

Remote rekeying: Procedure by which a distant cryptoequipment is rekeyed electrically.

Reserve on board (ROB): A quantity of keying material, not yet effective, held in reserve by an account for use at a later date.

Resident alien: A citizen of a foreign country who is legally residing in the United States on a permanent basis. (NOTE: Diplomatic personnel are not considered resident aliens.)

Running inventory (R/I): A list AL 1 through AL 4 COMSEC material held in a CMS account.

SECNAVINST 5720.42 (series): Department of the Navy Freedom of Information Act (FOIA) Program. (NOTE: Implements DON policies and procedures for handling FOIA requests and FOUO/unclassified information.)

Seed key: Initial key used to start an updating or key generation process.

SF-153: Multi -purpose form used to record COMSEC material transactions except for inventories (e.g., transfer, destruction).

Short title: A series of letters and/or numbers (e.g., KG -84, USKAT 2333), used for brevity, and assigned to certain COMSEC materials to facilitate handling, accounting, and control.

ANNEX A
GLOSSARY

SPCCINST 2300.4 (series): Utilization and Disposal of Excess Communications Security (COMSEC) and Signal Intelligence (SIGINT) Material. (NOTE: This instruction provides procedures for utilization, turn -in, and disposal of excess COMSEC and SIGINT material.)

SPCCINST 5511.24 (series): Classified Electronic Communications Security (COMSEC) Material in the Navy Supply System. (NOTE: This instruction provides procedures for the security accounting and inventory management control of classified electronic COMSEC material received and issued by the Navy Supply System.)

Staff CMS Responsibility Officer (SCMSRO): An individual (O -4 or above), designated by a flag or general officer in command status (or any officer occupying the billet of a flag or general officer with command status), responsible for the proper administration of routine CMS matters for a command's CMS account.

Start-up KEK: Key encryption key held in common by a group of potential communicating units and used to establish ad hoc tactical nets.

Status: Determines the usability of COMSEC material. (NOTE: COMSEC material is always in one of three status conditions: reserve, effective, or superseded.)

Supersession: Scheduled or unscheduled replacement of COMSEC material with a different edition. (NOTE: Supersession may be regular, irregular, or on an emergency basis.)

Telecommunications: Preparation, transmission, communication, or related processing of information (writing, images, sounds or other data) by electrical, electromagnetic, electromechanical, electro -optical or electronic means.

TEMPEST: Short name referring to investigation, study, and control of compromising emanation from telecommunications and AIS equipment.

Test key: Key, marked CRYPTO, intended for on -the-air testing of COMSEC equipment or systems.

Traffic encryption key (TEK): Key used to encrypt plain text or to superencrypt previously encrypted text and/or to decrypt cipher text.

ANNEX A
GLOSSARY

Training key: Key, not marked CRYPTO, intended for off-the-air training. (NOTE: Training key is restricted to off-the-air, in-classroom use only.)

Transaction log: Used to record and assign a six-digit number to transactions reportable to the DCMS COR.

Transaction number (TN): A number used to maintain continuity of CMS material transactions. There are two types of TNs: DCMS COR-reportable (e.g., receipts/transfers) and local (e.g., local custody receipts/issues, destructions).

Transmission security (TRANSEC): Component of communications security that results from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.

Transmission security key (TSK): Key that is used in the control of transmission security processes, such as frequency hopping and spread spectrum.

Two-Person Control (TPC): Continuous surveillance and control of positive control material and devices at all times by a minimum of two authorized persons, each capable of detecting incorrect or unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements.

Two-Person Integrity (TPI): A system of handling and storing designed to prevent single-person access to certain COMSEC keying material. (NOTE: TPI requires that at least two persons, authorized access to COMSEC material, be in constant view of each other and the COMSEC material requiring TPI whenever that material is accessed and handled. Each individual must be capable of detecting incorrect or unauthorized security procedures with respect to the task being performed.)

TPI storage: TPI storage requires using two approved combination locks (each with a different combination) with no one person authorized access to both combinations. (NOTE: Security containers approved for storage of COMSEC keying material are outlined in Chapter 5.)

Unique Variable (key) (UV): This key is used in conjunction with (A two other keys, the Broadcast Area Variable (BAV) and Community Variable (CV), for KW-46 secured broadcasts. More specifically, UVs are used to decrypt KW-46 BAVs as they are loaded into each using equipment. A separate UV is assigned to each U.S. Navy and U.S. Coast Guard ship or activity that copies any U.S. Navy KW-46 secured broadcasts.

ANNEX A
GLOSSARY

Updating: Automatic or manual cryptographic process that irreversibly modifies the state of a COMSEC key, equipment, device, or system.

User representative: Person authorized by an organization to order COMSEC keying material and to interface with the keying system to provide information to key users, ensuring that the correct type of key is ordered.

Violating command: The command, unit, or activity responsible for a reportable COMSEC incident or insecurity.

When directed (WHENDI): Term used to indicate that COMSEC material is not authorized for use or destruction until notified by the material's controlling authority.

Zeroize: To remove or eliminate the key from a crypto -equipment or fill device.

ANNEX B
COMMONLY USED ABBREVIATIONS AND ACRONYMS

A&A	advice and assistance
ACMS	Automated Communications Security Material System
ADM	advanced development model
ADP	automated data processing
ADPSO	Automated Data Processing Security Officer
AFEKMS	

COMMONLY USED ABBREVIATIONS AND ACRONYMS

CAC	codes, authenticators, and call signs
CAG	collective address group
CARS	COMSEC Automated Reporting System
CCEP	Commercial COMSEC Endorsement Program
CCI	controlled cryptographic item
CDP	command distribution precedence
CDR	critical design review
CDT	critical developmental testing
CEOI	Communications Electronics Operation Instruction
CIK	crypto -ignition key
CIM	1. compromised information message 2. Communications Improvement Memorandum
CIMA	COMSEC Incident Monitoring Activity
CITA	COMSEC Incident Trend Analysis
CKEK	contingency key encryption key
CKG	cooperative key generation
CKL	compromised key list
CLMD	COMSEC local management device
CM	configuration management
CMC	Commandant Marine Corps
CMCS	COMSEC Material Control System
CMIO	COMSEC Material Issuing Office
CMS	COMSEC Material System
CNCTC	Commander, Naval Computer & Telecommunications Command
CNO	Chief of Naval Operations
CO	Commanding Officer

ANNEX B

COMMONLY USED ABBREVIATIONS AND ACRONYMS

COI	1. course of instruction 2. community of interest
COMDT COGARD	Commandant, Coast Guard
COMNAVRESFOR	Commander, Naval Reserve Force
COMPUSEC	computer security
COMSC	Commander, Military Sealift Command
COMSEC	communications security
CONUS	continental United States
COR	Central Office of Record
COTS	commerical off -the-shelf
CPU	central processing unit
CRF	crypto repair facility
CRYPTO	cryptographic -related
CSP	COMSEC Publication
CSPM	COMSEC Publication Manual
CV	Community Variable (CV) (A
CVBG	Carrier Battle Group
CY	calendar year
D&A	distribution and allowance
DA	destruction automatic
DAO	Defense, Agency, Organization
DBES	disk based encryption system
DCMS	Director, Communications Security Material System
DCS	1. Defense Courier Service 2. Defense Communications Service
DDN	Defense Data Network

ANNEX B

COMMONLY USED ABBREVIATIONS AND ACRONYMS

DES	data encryption standard
DIRNSA	Director, National Security Agency
DM	destruction manual
DMR	date material required
DON	Department of the Navy
DSN	Defense Switched Network
DT	developmental testing
DTD	data transfer device
DT&E	developmental test and evaluation
DTG	date-time-group
EAM	emergency action message
EAP	emergency action plan
ED	edition
EDM	engineering development model
EFTO	encrypted for transmission only
EKMS	Electronic Key Management System
ELINT	electronic intelligence
ELSEC	electronic security
ENDEX	end exercise
ETR	electrical transaction report
EX	exercise
FC	fixed-cycle
FD	fill device
FEP	front-end processor

ANNEX B

COMMONLY USED ABBREVIATIONS AND ACRONYMS

FIFO	first-in-first-out
FLTCINC	Fleet Commander in Chief
FLTSAT	fleet satellite
FMF	Fleet Marine Force
FOUO	For Official Use Only
FSTS	Federal Secure Telephone Service
FTS	Federal Telecommunications System
FY	fiscal year
GENSER	General Service
GPS	Global Positioning System
GSA	General Services Administration
HCI	highest classification indicator
HDR	high data rate
ICP	Inter-theater COMSEC package
IDS	intrusion detection system
IFF	identification, friend or foe
ILS	integrated logistics support
INFOSEC	information security
IOC	initial operational capability
ISIC	Immediate Superior in Command
ISSA	interservice support agreement
IT	in-transit
JCEOI	Joint-Communication Electronics Operations Instruction
JKMS	Joint Key Management System

ANNEX B

COMMONLY USED ABBREVIATIONS AND ACRONYMS

JTIDS	Joint Tactical Information Distribution System
KAM	cryptographic maintenance manual
KAO	cryptographic operating manual
KCN	key conversion notice
KDC	key distribution center
KEK	key encryption key
KEYMAT	keying material
KG	key generator
KMC	key management center
KMS	Key Management System
KP	key processor
KPF	key production facility
KPK	key production key
KSD	key storage device
KVG	key variable generator
LAN	local area network
LCMS	local COMSEC management system (software)
LDR	1. local destruction record 2. low data rate
LH	local holder
LIFO	last-in-first-out
LMD	local management device
LMM	limited maintenance manual
LOA	1. letter of agreement 2. letter of appointment

ANNEX B

COMMONLY USED ABBREVIATIONS AND ACRONYMS

LOEP	list of effective pages
LOP	letter of promulgation
MARG	Marine Amphibiou s Ready Group
MATSYM	material symbol
MB	megabyte
MEU	Marine Expeditionary Unit
MIC	microfiche
MIUWU	Mobile Inshore Undersea Warfare Unit
MMVG	mandatory modification verification guide
MOA	1. memorandum of appointment 2. memorandum of agreement
MOS	metallic oxide semi -conductor
MOU	memorandum of understanding
MSE	mobile subscriber equipment
MTF	message text format
NACSI	National COMSEC Instruction
NACSIM	National COMSEC Information Memorandum
NATO	North Atlantic Treaty Organization
NCCD	nuclear command and control document
NCIRES	National COMSEC Incident & Reporting Evaluation System
NCS	1. National Communications System 2. net control station
NCTAMS	Naval Computer and Telecommunications Area Master Station
NCTS	Naval Computer and Telecommunications Station

ANNEX B

COMMONLY USED ABBREVIATIONS AND ACRONYMS

NES	Network Encryption System
NESP	Navy Extremely High Frequency (EHF) Satellite Communications Program
NKDS	Navy Key Distribution System
NLT	1. no later than 2. not later than
NLZ	no-lone zone
NSA	National Security Agency
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NSTISSD	National Security Telecommunications and Information Systems Security Directive
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NTISSI	National Telecommunications and Information Systems Security Instruction
OADR	originating agency's determination required
OIC	Officer-in-Charge
OPAREA	operating area
OPCODE	operations code
OPEVAL	operational evaluation
OPSEC	operations security
OTAD	over-the-air key distribution
OTAR	over-the-air rekeying
OTAT	over-the-air key transfer
OTC	1. over-the-counter 2. Officer-in-Tactical Command

ANNEX B

COMMONLY USED ABBREVIATIONS AND ACRONYMS

PAL	permissive action link
PASEP	passed separately
PC	personal computer
PD	pending destruction
PDS	1. practice dangerous to security 2. protected distribution system
PES	positive enable system
PLA	plain language address
PQS	personnel qualification standards
PROM	programmable read -only memory
PSTN	public switched tel ephone network
PWA	printed wiring assembly
QCCP	quick change card plate
RACE	rapid automatic cryptographic equipment
RAM	random access memory
RDT&E	research development test and evaluation
RI	1. running inventory (also appears as R/I) 2. routing indicator (also appears as R/I)
ROB	reserve -on -board
ROM	read -only memory
SA	system administrator
S&G	Sargent & Greenleaf
S/T	short title
SACC	special access control container
SAS	sealed authentication system

ANNEX B

COMMONLY USED ABBREVIATIONS AND ACRONYMS

SATCOM	satellite communications
SBI	special background investigation
SCA	STU-III COMSEC account
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SCMSRO	Staff CMS Responsibility Officer
SDNS	Secure Data Network System
SEPCOR	separate correspondence
SF	standard form
SI	special intelli gence
SIGINT	signal intelligence
SIGSEC	signals security
SINCGARS	single channel ground and airborne radio system
SIOP	single integrated operational plan
SOP	standard operating procedures
SQL	standard query language
SSIC	standard subject identification code
SSO	Special Security Officer
ST&E	security test and evaluation
STU	secure telephone unit
TECHEVAL	technical evaluation
TED	trunk encryption device
TEK	traffic encryption key
TFS	traffic flow security

ANNEX B

COMMONLY USED ABBREVIATIONS AND ACRONYMS

TN	transaction number
TPC	two-person control
TPI	two-person integrity
TRANSEC	transmission security
TRI-TAC	Tri-service Tactical Communications System
TSCM	technical surveillance countermeasures
TSCO	Top Secret Control Officer
TSEC	telecommunications security
TYCOM	Type Commander
UAS	user application software
UNODIR	unless otherwise directed
UR	User Representative
UV	Unique Variable (key) (A
VGA	video graphics array
WAN	wide area network
WETS	warehouse equipment tracking system
WHENDI	when directed
WWMCCS	Worldwide Military Command and Control System
XEU	Xerox Encryption Unit

ANNEX C

CONTROLLING AUTHORITIES FOR COMSEC MATERIAL

1. Purpose:

a. To describe the responsibilities and prerogatives of DON organizations performing controlling authority (CA) functions for COMSEC keying material.

b. This Annex also describes those functions and lists

ANNEX C
CONTROLLING AUTHORITIES FOR COMSEC MATERIAL

d. Specifies the key -change time when it is not stated in the keying material format. The selected time must be consistent throughout the cryptonet and chosen to have the least operational impact.

e. Recommends changes in system design (e.g., the content or format of the keying material). Submits recommendations to DIRNSA//V27/Y13// via DCMS//30// and the operational chain of command.

f. Makes spare group assignment in operations codes, as required.

g. Authorizes, in a non -emergency situation, local reproduction of keying material normally held by an account when the Letter of Promulgation or the Handling Instruction of the material involved does not provide holders the authority to prepare reproduced copies.

h. Reports faulty keying material (i.e., production error s) (R to DIRNSA//Y13/V51A// and info DCMS//20//. Directs holders to keep faulty keying material until disposition instructions are received from DIRNSA.

i. Ensures that faulty keying material, when directed to be returned for forensic examination by DIRNSA, is sent via DCS or the Diplomatic Courier Service to NSA account 880099, Operations Building #3, Fort George G. Meade, MD., 20755 -6000.

j. Initiates and conducts an annual review of all systems controlled to confirm there is a continuing requirement for the keying material in present quantity and reports the results to DCMS//30//, info DIRNSA//Y13//. Review efforts should focus on the following:

(1) Identification of large cryptosystems of low peacetime use that could be placed in contingency status.

(2) Deactivation of a cryptonet/circuit when it is no longer needed.

(3) Reserve keying material is adequate for unexpected cryptonetting requirements.

(4) Review of keying material for manual cryptosystems.

k. Assesses the security imp act of reports of physical incidents of superseded, effective, and future cryptonet keying material held, and determines whether or not a compromise of the material has occurred.

ANNEX C

CONTROLLING AUTHORITIES FOR COMSEC MATERIAL

NOTE: Chapter 9 contains procedures for reporting COMSEC incidents and provides guidance for assessing compromise probability.

l. When a compromise is declared, notify the cryptonet members and DCMS//30//, and info DIRNSA//V51A//. (R

m. Directs e mergency supersession of cryptonet keying material when required. Supersessions **must** be coordinated with DIRNSA//Y13// and appropriate distribution authorities (e.g., DCMS//30//). Notifies the appropriate distribution authorities of changes in status or implementation date.

n. DCMS and NSA must consider the following factors when directing emergency supersession:

(1) The number of editions held in reserve at the user level.

(2) The ability of DIRNSA to produce additional keying material and the ability of distribution authorities to supply replacement editions in a timely manner.

(3) The time required to notify all cryptonet members in advance of implementing date.

(4) The time required for the members to implement the new material.

4. Evaluating Reports of COMSEC Physical Incidents Involving COMSEC Keying Material:

a. Guidelines for Evaluating COMSEC Physical Incidents . COMSEC incident evaluation is often a subjective process, even when the CA is in possession of all pertinent facts. (**NOTE:** See Article 980 for guidance on assessing compromise probability.)

b. Time Limits for Evaluating COMSEC Incidents .

CAs are responsible for soliciting any information required to make an evaluation. COMSEC incident reports must be evaluated within the time limits specified below based on the precedence of the initial report. Time limits begin with receipt of the initial report, or amplifying report if the initial report does not contain sufficient information to permit an evaluation.

ANNEX C

CONTROLLING AUTHORITIES FOR COMSEC MATERIAL

Message Precedence	Response Time
IMMEDIATE	24 Hours
PRIORITY	48 Hours
ROUTINE	5 Working days

c. Action Required When COMSEC Keying Material has Been Compromised or Suspected Compromised . Where substantial evidence exists that COMSEC keying material has been compromised, the CA must first coordinate with DCMS//30// and DIRNSA//Y13// before directing supersession action. This coordination is necessary so that resupply action can be initiated. CAs will direct traffic reviews of record traffic encrypted in compromised keying material when warranted.

(1) Superseding electronically generated key presents a unique problem for mobile/tactical users in that some of the communications paths used to deliver the key may no longer exist, because some of the relaying units may have redeployed and can no longer serve in that capacity. Consequently, before directing supersession action, CAs must take into consideration the time needed to create or reestablish communications paths.

(2) When precautionary supersession is warranted but not all net members hold or cannot be supplied with replacement key via normal logistic channels, the following options are available to the CA:

(a) OTAR/OTAT.

(b) Direct the early implementation of uncompromised future editions by those cryptonet members who hold those editions or can be supplied quickly, and exclude from net operations those members who do not hold or cannot be furnished the replacement material.

(c) Physically transfer key to net members in a fill device (FD). When keyed, FDs must be afforded protection at the same classification of the key they contain.

(3) When supersession is warranted but not feasible, the following options are available to the CA:

ANNEX C
CONTROLLING AUTHORITIES FOR COMSEC MATERIAL

(a) Extend the cryptoperiod of uncompromised keying material as follows:

1 Off-line systems (e.g., call sig ns, operational codes, authenticators) up to 72 hours.

2 Automanual/machine cryptosystems (e.g., KL-43, KL-51, KG-81, KG-84, KG-94, KY-57/58, KY-65/75) up to one (1) week.

NOTE: NCSs and net subscribers may exceed these cryptoperiod extensions up to two hours to complete a transmission in progress at key change time. Authorization to further extend cryptoperiods must be submitted to DCMS//20//, info to DIRNSA//V5//. CAs are not required to report these extensions to N SA or DCMS. (R

(b) Suspend cryptonet operations until key can be resupplied.

(c) Continue to use compromised key. This action is a **last** resort when normal supersession of the compromised material will take place before emergency supersession can be accomplished, or where keying material changes would have a serious detrimental effect on operations, or where replacement material is not available.

1 The CA must alert net members (by other secure means, if available) that a possible compromise has occurred and direct that members minimize transmissions using the compromised key.

2 This option should be resorted to only when continued cryptonet operation is critical to mission accomplishment.

5. Designating Contingency Keying Material:

a. When large amounts of crypto materials are provided for regular consumption, and are destroyed unused, the CA should consider placing the material into contingency status.

b. Contingency keying material is material held for use under specific operational conditions or in support of specific contingency plans.

c. The material is not activated until needed for the specific requirement, and is not destroyed until after use.

ANNEX D

COMMUNICATIONS SECURITY MATERIAL SYSTEM (CMS) FOR COs

1. Introduction:

a. Experience has shown that where there is command involvement in the operation and administration of a CMS account, the end result is efficiency in cryptographic operations and fewer COMSEC incidents and insecurities.

b. The information contained in this Annex is provided as a tool for assisting COs, OICs, and SCMSROs in the management oversight of their respective CMS account.

2. Selecting Custodian Personnel:

a. The selection of personnel to serve as CMS Custodian and Alternate(s) should be made carefully. In making your selections, consider the sensitivity and criticality of the communications being protected by the materials you will be entrusting to your Custodian personnel.

b. An error on the part of a Custodian who is assigned too many duties, or who is poorly trained, poorly motivated, or otherwise not suited for the job, can negatively impact mission fulfillment or jeopardize untold amounts of extremely sensitive information.

3. COMSEC Incident Reporting:

a. The COMSEC system has been designed to provide a means for taking corrective action when deviation from established policy and procedures has occurred.

b. These deviations may jeopardize or have the potential to jeopardize national security. However, unless those who handle and manage COMSEC material report deviations specifically identified as COMSEC incidents in a timely manner, corrective actions cannot be implemented. Consequently, you play a vital role in this process.

4. Resource Assistance: A variety of services and aids are at your disposal to help you prepare for formal inspections, resolve CMS issues, obtain interpretation of CMS policy and procedures. These include:

a. FLTCINC/TYCOM/ISIC/CMS A&A Training Team: When in doubt about a CMS matter, encourage your Custodian to contact your CMS FLTCINC/TYCOM/ISIC representative or if unavailable, the nearest CMS A&A Training Team. (NOTE: See Chapter 3 for assistance/ services provided by CMS A&A Training Team personnel.) These are

valuable resources and should be used to the maximum extent possible.

b. DCMS: If the ISIC or CMS A&A Training Team is unavailable or additional assistance is required, contact DCMS//20//, CMS Policy and Procedures, or //80//, CMS Education and Training.

c. CMS UPDATE: This newsletter is published bi-monthly by DCMS and distributed automatically to all established CMS Accounts. This newsletter addresses a wide variety of CMS-related information, including useful account management advice, interpretation of CMS policy and procedures, and security awareness information.

5. Unannounced Spot Checks:

a. A spot check must be conducted at least quarterly, but more frequently is strongly encouraged. Ensuring that unannounced spot checks are conducted has proven to be of significant value. Potential problems can be identified and corrective measures taken prior to an official inspection.

NOTE: COs may delegate no more than two of the four quarterly spot checks to the Executive Officer.

b. The checklist provided in Tab 1 to this Annex can be used to assess command compliance with proper CMS policy and procedures. Additionally, a more comprehensive "Spot Check" form is available from your cognizant CMS A&A Training Team.

NOTE: All references listed in the checklist refer to CMS 1 unless otherwise indicated.

ANNEX D

CMS ACCOUNT ASSURANCE CHECKLIST

YES	NO	
___	___	1. Have Letters of Appointment been prepared for all Custodian personnel and, if appointed, for the CMS Clerk? Are they filed in the Correspondence/ Message File (Article 425 and Annex J)
___	___	2. Has a CMS Form 1, Authorization to Receipt for and Courier COMSEC Material, been completed and forwarded to your servicing CMIO? (Annex I) **NOTE: ONLY** required if a command will pick up material at a CMIO.
___	___	3. For Local Holders who are responsible to a different Commanding Officer than the CMS account command, have Letters of Agreement between the Commanding Officers been completed? (Article 445 and Annex L)
___	___	4. Do the CMS Custodian and Alternate(s), Local Holders and Alternate(s), and the CMS Clerk (if appointed) meet designation requirements ? (Article 415 and 420)
___	___	5. Does the CMS Custodian keep the Alternates informed of the status of the account at all times? (Article 455.d.)
___	___	6. Has the Personnel Qualifications Standards (PQS) (NAVEDTRA 43462 (series)) for CMS been incorporated into the command's training program for CMS personnel (less USCG/USMC personnel)? (Article 450 e.)
___	___	7. Has the Custodian established the required CMS Account Files, Records, and Logs? Are they properly classified? And are they retained for the required time period? (Chapter 7 and Annex T)

a. CMS Chronological File (Article 706)
b. CMS Correspondence, Message, and Directives File (Article 709)
c. CMS Local Custody File (Article 712)

___	___	8. Is the Custodian maintaining the account's portion of the command Emergency Action Plan (EAP)? (Annex M)

ANNEX D

CMS ACCOUNT ASSURANCE CHECKLIST

YES	NO		
___	___	9.	Are amendments to COMSEC publications properly entered, recorded, and the residue properly destroyed? (Article 787)
___	___	10.	Are the CMS Transaction Log and Running Inventory current? (Annex U and Z)
___	___	11.	Are receipts for CMS material submitted by the command in a timely manner? (Article 742)
___	___	12.	Are authorized destruction methods being used for paper and non-paper COMSEC and CMS-related materials? (Article 540)
___	___	13.	Are destructions conducted within the proper timeframes? (Article 540)
___	___	14.	Are the original SF 153 monthly destruction reports signed by the Custodian (or Alternate), a properly cleared witness, and the Commanding Officer (or SCMSRO/OIC)? (Annex V)
___	___	15.	Are CMS 25 and other Lo cal Destruction Reports (i.e., SF 153 or locally prepared equivalent) signed by at least two authorized personnel? (Chapter 7 Figures 7-1 through 7-3)
___	___	16.	What are the account's fixed-cycle inventory dates? Are inventories being conducted in accordance with those dates and are the results of those inventories being reported to DCMS as required? (Article 766 and Annex AA)
___	___	17.	Are the results of Local Holder and User Inventories forwarded to the Accou nt Custodian for his/her use in completing entries on the account command's DCMS-generated SF 153 Inventory? (Article 766)
___	___	18.	Is proper storage available for the command's COMSEC materials? Specifically, is classified keying material marked CRYPTO stored under TPI? (Article 510)

ANNEX D

CMS ACCOUNT ASSURANCE CHECKLIST

YES	NO	
___	___	19. Are the COMSEC Incident reporting requirements understood by all personnel who use and handle COMSEC material? Is the question of "who" must report clearly outlined in any Letters of Agreement generated between this command and any others? (Article 445, Chapter 9, and Annex L)
___	___	20. Is there a record of all COMSEC security container combinations on file in the event of an emergency? Are the combinations to the account's TPI containers properly stored and sealed? (Article 515)
___	___	21. Are CMS A&A Training Team visits being requested at the required intervals? (Article 315)

TAB 1

ANNEX E
COMSEC MATERIAL STATUS REPORT (CMSR)

```
                    COMSEC MATERIAL STATUS REPORT   (CMSR)
                              09   -AUG-1994  19:00

                       MASTER  COMSEC  MATERIAL  LISTING

                                          Effect     Disp        Disp
    S/T  Designator Edition        Amend   Date       Date        Code   ALC
        ------------ -------         -------  -------    -------     ------ ----

    AKAT  23235     Description:  KG   -84 A/C Operational OTAR KEK Keytape    Class:   T    Area:   WP
                    Cntrl  Auth:  NCTAMS  EASTPAC  HONOLULU  HI             Effect Period:   1YR
                     Remarks:

                    H                       19930601   19940601    DAL    1

    AKAT  34346     Description:  KG   -84 Operational Keytape                Class:   S    Area:   WW
                    Cntrl Auth:   DCA  WASHINGTON  DC                        Effect Period: 1YR
                    Remarks:

                    A                       WHENDI                 DAL    1
                    B                       WHENDI                 DAL    1

    AKAT  45457     Description:     KG-84  A/C  Operational  OTAR KEK  Keytape Class:   S    Area:  EP
                    Cntrl  Auth:  NCTAMS  EASTPAC  HONOLUL HI                Effect Period: 1M
                    Remarks:

                    E                       19940901   19941001    DAL    1
                    F                       19941001   19941101    DAL    1

    Class:   T  =  Top Secret      S  =  Secret      C  =  Confidential      U  =
Unclassified
    ALC:     1  =  AL1        2  =  AL2        3  =  AL3        4  =        AL4
    Area:    A  =  Atlantic      P  =  Pacific      WW  =  Wordlwide      WP  =
Westpac      EP  =  Eastpac
             M  =  Mediterranean      IO  =  Indian  Ocean
```

1. General:

a. The COMSEC MATERIAL STATUS REPORT (CMSR) (i.e., the former CSPM MIC -3), is classified SECRET NOFORN, is produced in two forms and can be viewed and/or downloaded via CARS:

(1) The Master CMSR (MCMSR) lists **ALL** COMSEC material distributed to DON CMS accounts. This report will be updated twice a week. Accounts should **NOT** attempt to download the MCMSR due to its length. For example, tests have shown that it takes approximately four (4) hours (at 9600 baud) to download the MCMSR.

(2) The Customized CMSR (C2MSR) lists only COMSEC material that the DCMS database reflects as held by an individual account as of the date of the report. This report will be updated at the beginning of each month by the fourth business day and can be downloaded via CARS to an account's PC .

ANNEX E

COMSEC MATERIAL STATUS REPORT (CMSR)

(a) A C2MSR can be updated more often by calling your servicing DCMS team in 30 Department. Within three (3) working days of your request, the C2MSR will be updated and available for viewing and/or downloading via CARS.

(b) Do **not** "reset" or retain a C2MSR in your mailbox after it has been downloaded via CARS. If a C2MSR is retained after it has been downloaded, you may receive out of date status information due to processing features within the FEP/NKDS.

NOTE: Use of the MCMSR is limited to viewing to determine the most current status information. The C2MSR, however, may be viewed and/or downloaded.

b. The MCMSR is to be used **in conjunction with** any messages from controlling authorities throughout the month for the most current COMSEC material status information and prior to conducting destruction of COMSEC material. In the event of conflicting information, destruction is to be based on the most current information. Guidance may also be obtained from DCMS//30//.

c. On each page of the CMSR, immediately below the report name, you will see a date and time. This information reflects the status of the short titles on that page as of that date and time.

2. **CMSR Access Via CARS**: The CMSR is only available via CARS. Use the procedures in Annex F to access CARS. To view all of the data for a short title on the CMSR, the monitor width must be set to "132" characters using the procedures in Tab 2 of Annex F.

3. **Content**: Each short title of COMSEC material listed on the CMSR will provide the following information:

a. Edition,
b. Amendment,
c. Effective date (e.g., 19940901)
d. Disposition date, (e.g., 19950101)
e. Disposition code (e.g., DAL)
f. Accounting legend code (ALC),
g. Description of the short title,
h. Controlling authority,
i. Classification,
j. Area of use, and
k. Effective period of the short title.

ANNEX E

COMSEC MATERIAL STATUS REPORT (CSMR)

NOTE: A legend for the classification, ALC, and area of use is provided at the bottom of each page of the CMSR.

4. **Short title explanations**: The following explains the short titles on the example page of a CMSR presented earlier:

a. The first short title example, AKAT 23235 edition "H" is classified TOP SECRET, is used in Westpac, and has an effective period of one (1) year. This short title is authorized for destruction 19940601 (i.e., Jun 1, 1994).

b. In the second short title example, none of the editions of AKAT 34346 are authorized for use. The "WHENDI" (when directed) means that until the controlling authority (DCA WASH) notifies all holders of the date that each edition is effective for use, the material must not be used.

c. In the third short title example, AKAT 45457 edition "E" is effective on 1 Sep 94 and is authorized for destruction on 1 Oct 94. Edition "F" is effective 1 Oct 94 and is authorized for destruction on 1 Nov 94.

5. **Effective period**: Terms used to indicate the effective period are as follows:

a. D: Preceded by a number which indicates the number of days the edition is effective (e.g., 3D, 10D, 15D).

b. M: Preceded by a number which indicates the number of months the edition is effective (e.g., 1M, 2M, 3M).

c. Y: Preceded by a number which indicates the number of years the edition is effective (e.g., 1YR).

NOTE: Disregard any other letters other than D, M, and Y. If the "Effect period" field is blank, the effective period is indefinite or not known.

6. **Disposition Codes**: **Prior** to destroying any COMSEC material listed on the CMSR, the disposition codes listed in the "disp code" column must be reviewed and followed. Disposition codes and their instructions are as follows:

a. **DAL** -- All accounts destroy.

ANNEX E

COMSEC MATERIAL STATUS REPORT (CSMR)

b. **DAZ** -- Retain until receipt of successor edition; upon receipt of successor edition, destroy. Accounts whose current operation orders indicate the successor edition will not be required (e.g., shipyard overhaul and/or material removed from the account allowance), are authorized to destroy the old edition without receipt of the successor edition.

c. **DEQ** -- Disposition guidance will be provided by DCMS upon request from the user command.

d. **DHL** -- Accounts 100000 -399999, destroy amendment residue after entering amendment. CMIOs and DCMS retain unentered amendments.

7. **C A U T I O N**: **NEVER** destroy COMSEC equipment without specific written guidance from DCMS//30//, except in case of emergency destruction.

COMSEC AUTOMATED REPORTING SYSTEM (CARS)

1. **General:**

a. CARS is a communications system that provides the capability for electronically viewing data at DCMS (e.g., COMSEC Material Status Report (CMSR), CMS Update), sending electronic or E-mail to DCMS, and transferring files to and from DCMS. Access at DCMS is via a STU -III, keyed with SECRET key only and a front-end-processor (FEP) which is cleared for SECRET.

b. The CARS facilitates the exchange of data/text that is in the form of an ASCII file via a personal computer (PC) and a STU-III (with its internal modem).

c. Data fields for reporting COR -reportable transactions (e.g., receipts and transfers) are constructed using the formatting requirements for an Electrical Transaction Report (ETR) which are contained in Annex W.

d. The ANCRS program automatically and correctly formats ETRs for transmission via CARS only. ANCRS -generated ETR data fields may also be inserted into the text of a message and forwarded via the General Service (GENSER) AUTODIN Communications Network using Message Text Format (MTF) Editor or an authorized word processing software package.

NOTE: Annex AB contains a list of software that is authorized for use on the LMD.

e. **KEYBOARD ENTRIES ON THE FEP ARE CASE SENSITIVE** (i.e., upper case or lower case letter entries must be entered exactly as shown in file names (including file name extensions) or as you entered your password).

f. CARS and ANCRS lead the way for the Navy Key Distribution System (NKDS) which will, in its final phase, fully automate most COMSEC functions and provide for the electronic generation, distribution, and accounting of COMSEC key at all levels of command.

2. **CARS Capabilities**. CARS is an interactive system with the following menu -selectable options:

ANNEX F

COMSEC AUTOMATED REPORTING SYSTEM (CARS)

a. **Change Password**: Permits users to change their password. (**NOTE**: Passwords automatically expire after 90 days.)

b. **Download files**: Allows users to transfer files from DCMS to their PC. This could be an SF -153 Inventory or the Customized COMSEC Material Status Report (C2MSR).

c. **Goodbye**: Logs you off the CARS FEP.

d. **List files available**: Lists files in an account's mailbox that can be viewed and/or downloaded to their PC.

e. **Mail file**: Permits users to send E -mail to specific mailboxes at DCMS.

f. **File reset**: Allows users to retain files in their mailbox after they have been downloaded to their PC.

g. **Upload files**: Permits users to transfer ASCII ETR files from their PC to DCMS.

h. **View files**: Allows viewing of files in an account's mailbox. Selecting this option will also allow you to enter a "string" of characters and search for a match in the file being viewed (e.g., MCMSR or C2MSR, CMS Update).

3. **Minimum Hardware Requirements:**

a. An IBM or IBM -compatible PC (80286 minimum) with 640K RAM, VGA color monitor (preferably) or monochrome monitor, 20MB hard disk, 5 1/4" floppy disk drive, 1 printer port, 2 serial ports, and MS -DOS (Version 3.21 or higher).

b. A dot -matrix printer for printing files/documents.

c. A STU -III which functions a s the crypto device and the communications MODEM during the exchange of data.

d. RS-232 cable (i.e., serial printer cable) for connecting the STU -III to the PC.

ANNEX F

COMSEC AUTOMATED REPORTING SYSTEM (CARS)

4. **Software Requirements**:

a. ONLY those software programs listed in Annex AB are authorized for installation and use on the Local Management Device (LMD) (i.e., the personal computer distributed to all DON CMS
accounts at direction of CNO).

b. The electronic exchange of information via CARS requires PROCOMM PLUS (PCPLUS) communications software and, ANCRS or an authorized word processing software package. If ANCRS is not used, the word processing software must be capable of converting text to an ASCII file prior to transferring the file via CARS.

c. Software options and available sources are as follows:

(1) **WORD PROCESSING**:

(a) Commercial o ff-the-shelf (COTS) word processing packages that will convert a text file to an ASCII file. These packages are available from various vendors and/or the command software representative.

(b) Message Text Format (MTF) Editor may be used as it also has the capability to generate an ASCII file.

1 MTF Editor is an easy -to-use message preparation tool that generates, formats, and permits editing of USMTF formatted messages, General Administrative (GENADMIN) messages, non -GENADMIN messages a nd free text messages. MTF Editor is certified for joint use.

2 MTF Editor is available at NO COST from any NCTS or NCTAMS communications center. The software can also be downloaded to your PC by calling NCTS San Diego at COMM: (619) 545-0167 or DSN: 735 -0167. If additional information is needed, call the MTF Service Desk at COMM: (619) 735 -8686 or DSN: 735 -8686.

NOTE: If MTF Editor is used, the message heading/preamble lines must be removed prior to transmitting an ETR via CARS to ensure correct processing at DCMS (i.e., the FEP only recognizes the ETR data fields; any extraneous data/info will result in the ETR being routed to an error queue).

ANNEX F

COMSEC AUTOMATED REPORTING SYSTEM (CARS)

(c) ANCRS users that transmit their ETRs via CARS, will not require word processing software since ANCRS automatically and correctly formats ETR data fields into an ASCII file acceptable for transmission via CARS.

(2) **COMMUNICATIONS**:

To gain access to the FEP at DCMS, accounts must use the "PROCOMM PLUS" (PCPLUS) communications software. This software can be obtained (free) by calling the LMD Hotline at 800 NKMS-201 OR COMM: (803) 552 -0926/8538.

NOTE: Install PCPLUS using the guidance/procedures contained in its documentation package. Ensure that back -up copies of the program are made and stored in a safe location in the event of disk and/or PC problems.

5. **CARS Account:**

A CARS account m ust be established **before** attempting to access the database at DCMS. Once a CARS account is established, access to CARS is permissible at any time. The following

ANNEX F
COMSEC AUTOMATED REPORTING SYSTEM (CARS)

This single number is for all users and is connected to a rotary telephone system containing twenty (20) lines.

c. COMPUSEC rules prohibit access to CARS using a PC approved for processing Top Secret, Confidential, or Sensitive Compartmented Information/Special Intelligence (SCI/SI).

d. SCI/SI facilities may face some constraints. CMS Custodians must consult with both their command ADP Security Officer (ADPSO) and Special Security Officer (SSO) to obtain authorization to exchange data via CARS.

7. **ETR Formatting Procedures/Requirements:**

a. ETRs consists of precisely -formatted data fields that permit automated processing by the DCMS COR computer. Short titles are formatted the same way as they appear on inventory reports. ETRs must be transmitted via CARS, or as an alternative, in message format, via AUTODIN ONLY when access to CARS is not possible.

b. Annex W contains procedures for formatting ETRs for commands exempt from using ANCRS and the requirements for submitting ETRs in message format via AUTODIN.

8. **Conversion to an ASCII File:**

All information (i.e., ETRs, E-mail) forwarded to DCMS via CARS must be an ASCII file. If an ASCII editor program is not used, consult your software documentation for instructions on converting non-ASCII text files to ASCII. ETRs generated by ANCRS are in the correct format for transmission via CARS and will not require any conversion.

9. **STU-III Preparation:**

a. The STU-III must be configured with the following data communications settings:

(1) 2400 - 9600 baud
(2) Full Duplex
(3) Asynchronous

b. Then insert the STU-III Crypto Ignition Key (CIK) into the STU-III and connect the STU-III to the PC using standard RS-232 cable. (**NOTE**: Ensure that the ADPSO, and the SSO (for SCI/SI facilities) have provided authorization to connect a STU-III to a PC.)

ANNEX F
COMSEC AUTOMATED REPORTING SYSTEM (CARS)

NOTE: When accessing CARS, do NOT use the dialing directory within the PCPLUS program. Dial the CARS FEP access phone number using the STU -III.

10. **Records Requirements**:

a. Retain transmitted files (e.g., transfer/receipt ETRs) on disk until a subsequent SF -153 Inventory from DCMS indicates that the DCMS database processed the ETRs correctly.

b. Annotate on the applicable CMS document (e.g., SF 153) that the transaction has been reported to DCMS via CARS on YYMMDD (e.g., 940817) and file the document in the CMS Chronological File.

11. **CARS Assistance and Procedures for Accessing CARS:**

a. Annex F Tab 1 contains logon procedures and information necessary to execute the various options available when accessing the CARS FEP.

b. In order to view the CMSR, your monitor width must be set to "132." Tab 2 to this Annex contains the procedures for changing the column width from 80 to 132 characters.

c. In the event you cannot access the CARS FEP or need assistance, contact the DCMS CARS POC, Mr. Wayne Smith, at:

COMM: (202) 764 -0704/0856 DSN: 764 -0704/0856

12. **Summary of Steps Required to Process Data Via CARS:**

a. Obtain required hardware and software.
b. Obtain authorization from ADPSO, and the SSO (for SCI/SI facilities) to connect a PC to a STU -III.
c. Establish a CARS account with DCMS//50//.
d. Format data fields using ANCRS or ETR formatting procedures (Annex W).
e. Convert text/data fields to an ASCII file (if necessary).
f. Connect STU -III to PC and set STU -III data communications settings.
g. Configure your system using PCPLUS.
h. Dial CARS access telephone number from your STU -III keypad .
i. Log on to CARS.
j. Transfer and/or view file(s).
k. Log off of CARS.

ANNEX F - TAB 1
ACCESSING THE COMSEC AUTOMATED REPORTING SYSTEM (CARS)

1. General:

a. CARS is a SECRET system and can only be accessed using a PC cleared for SECRET and a STU-III keyed with SECRET key only.

b. The information herein details the procedures for logging onto CARS and guidance for executing the available options within CARS. Beginning with the CARS LOGON SCREEN, each option, in order of its appearance on the MAIN MENU SCREEN, is presented. Directly below each screen you will find the guidance/procedures for using that option.

2. Log on Procedures for CARS:

a. At the DOS prompt (e.g., C>, C:) on your PC, type "CD PCPLUS" to change to the directory where the PCPLUS software is installed. Type "PCPLUS" and then press "ENTER/RETURN."

b. A status line similar to the one below will appear:

ALT-Z FOR HELP I VT102 I FDX I 9600 N81 I LOG CLOSED I PRINT OFF I OFF-LINE

c. If the status line does not appear as indicated above, or you want to alter the settings (e.g., baud rate), press "**ALT P**." Settings should be as follows:

(1) PC Comm Port = 1 (if using Comm 1) or 2 (if using Comm 2)
(2) Baud rate = from 2400 to 9600 (set according to the baud rate of your STU-III)
(3) Data bits = 8
(4) Parity = N
(5) Stop bits = 1

NOTE: After your selections are made, press "**ALT S**" to save the settings. The revised settings should remain as the default settings in PCPLUS and the updated status line will appear on the screen.

(6) Terminal type = VT100 or VT102 (either one can be used)

NOTE: To change terminal type press "**ALT S**" and then select "TERMINAL OPTIONS," press "**A**" (for terminal emulation), highlight "VT/ANSI" and press "ENTER/RETURN." Select either VT100 or 102 and press "ENTER/RETURN" followed by pressing the "ESC" key. Next, select "SAVE SETUP OPTIONS" and press "ENTER/RETURN" followed by the "ESC" key.

d. After configuring your system, from your STU -III, (do **NOT** use the dialing directory within PCPLUS), call COMM: (202) 764-0340 or DSN: 764 -0340.

e. Once the connection to the CARS FEP is made, the status line at the bottom of the screen will appear as:

ALT-Z FOR HELP I VT102 I FDX I 9600 N81 I LOG CLOSED I PRINT OFF I **ON-LINE**

f. Next, the CARS LOGON SCREEN should appear with the "login" prompt at the bottom left -hand corner of the screen as shown below.

CARS LOGON SCREEN

login:

********** **USER GUIDANCE** **********

1. The CARS LOGON SCREEN is the initial screen that will appear when you access the CARS FEP. This is where you will access the database at DCMS after entering your logon ID and password.

2. Login ID : All logon IDs on the FEP will be your CMS account number. If your Login ID is preceded by a letter, the letter will be an "UPPER" case letter (e.g., A123456). If you attempt to login with a lower case letter "a123456", your login will fail and you will be prompted to reenter your User Name. Your User Name is the same as your Login ID. Type your **"LOGIN ID"** and press **"ENTER/RETURN"**.

3. Password guidance :

a. Passwords must have a minimum of six (6) and no more than eight (8) alphanumeric characters. Passwords may consist of letters and/or numbers. Ensure that your password is correctly entered (i.e., keyboard entries on the FEP are case sensitive; for example if your password is "ABC345," then "aBC345" will not work).

b. Protect your password just as a safe combination is protected because the password allows access to SECRET information in the database at DCMS.

c. Passwords automatically expire after ninety (90) days.

d. Use of profanity as part of a password or as a password is strictly prohibited .

4. Next, type your "password" and press "**ENTER/RETURN**." After a successful log on, the MAIN MENU SCREEN will appear as shown on the next page.

5. The following pages show the primary screens and provide instructions for using the options in the CARS FEP.

CARS MAIN MENU SCREEN

acct# Abc123 CARS Main menu

<C> Change password
<D> Download file
<G> Goodbye (log out to process files)
<L> List files available
<M> Mail file
<R> Reset file
<U> Upload file
<V> View file

C,D,G,L,M,U,V:

ALT-Z FOR HELP I VT102 I FDX I 9600 N81 I LOG CLOSED I PRINT OFF I ON -LINE

********** **USER GUIDANCE** **********

1. The MAIN MENU SCREEN appears after initially logging on to the CARS FEP. The CARS FEP will display your account number in the upper left -hand corner of the screen and a list of options which the user may select. These options include:

a. **C**hange user password.

b. **D**ownload or receive files from DCMS .

c. **G**oodbye (i.e., log off of CARS). Any file(s) uploaded will be sent to NKDS for processing at this time.

ANNEX F - TAB 1

ACCESSING THE COMSEC AUTOMATED REPORTING SYSTEM (CARS)

d. **L**ist will display the names of all files in your mailbox.

e. **M**ail file (i.e., send E -mail to DCMS).

f. **R**eset File (this feature allows you to retain account-specific files in your mailbox after they have been download to your PC).

g. **U**pload or transfer files to DCMS (ETR files only).

h. **V**iew files in your mailbox.

2. Enter the corresponding letter of the desired option to proceed.

3. The following pages show the screens for each of the above options and instructions for utilizing them within the CARS FEP.

CHANGE PASSWORD SCREEN

acct# Abc123 **Main menu**

<C> Change password
<D> Download file
<G> Goodbye
<L> List files available
<M> Mail file
<R> Reset file
<U> Upload file
<V> View file

C,D,G,L,M,U,V: C

Setting password for user: (name of account)
Enter current password:
New password:
Verify password:

ALT-Z FOR HELP I VT102 I FDX I 9600 N81 I LOG CLOSED I PRINT OFF I ON -LINE

ANNEX F - TAB 1

ACCESSING THE COMSEC AUTOMATED REPORTING SYSTEM (CARS)

********** **USER GUIDANCE** **********

1. Password guidance:

a. A password cons ists of a minimum of six (6) and a maximum of eight (8) alphanumeric characters. Passwords may consist of letters and/or numbers. Ensure that your password is correctly entered (i.e., keyboard entries on the FEP are case sensitive; for example, if your password is "ABC345," then "aBC345" will not work.

b. Protect your password just as a safe combination is protected since the password allows access to SECRET information in the database at DCMS.

c. Passwords automatically expire after ninety (90) days.

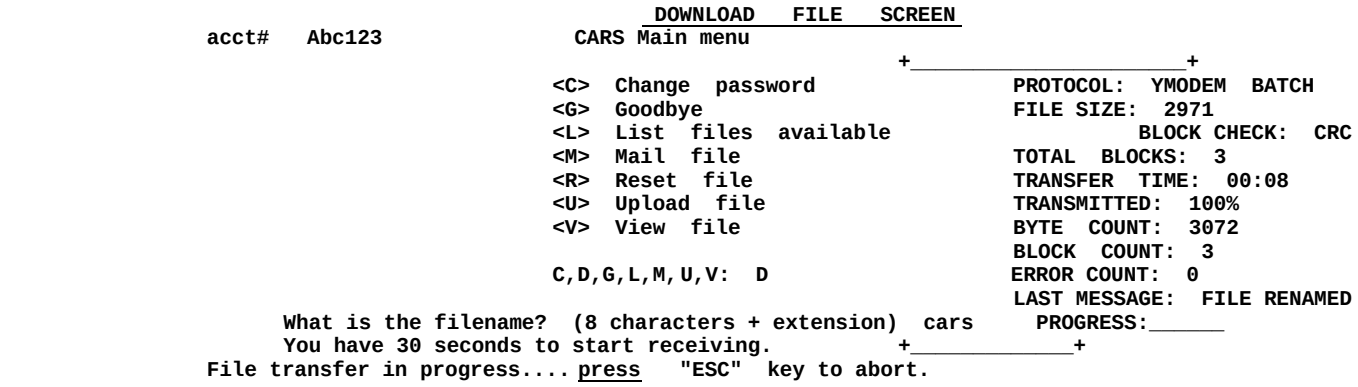
d. Use of profanity as part of a password or as a password is strictly **prohibited**.

2. Type "**C**" to change your password. Enter your current password and press " **ENTER/RETURN**."

3. The system will then prompt you to enter your new password. Enter your new password and press "**ENTER/RETURN**."

4. Next, the system will prompt you to re -enter your new password for verification. Re -enter your new password and press "**ENTER/RETURN**."

5. The system will then return you to the **MAIN MENU SCREEN**.



ANNEX F - TAB 1

ACCESSING THE COMSEC AUTOMATED REPORTING SYSTEM (CARS)

********** **USER GUIDANCE** **********

1. Selecting the " **D**" (i.e., download file) option allows you to transfer ASCII files from DCMS to your PC.

2. Prior to selecting the "D" option, you must know the name of the file you want to download. The names of files available for downloading can be obtained by selecting the "L" (i.e., list files available) option.

3. Type "**D**" to proceed and the system will prompt you for the filename that you want to download to your PC. Enter the filename exactly as it is shown and press "**ENTER/RETURN**."

4. The system will indicate that yo u have thirty (30) seconds to start receiving. At this time you will need to invoke or commence the download function of PCPLUS by pressing "page down" and then pressing "**Y**" (for YMODEM (batch)).

NOTE: To change/locate the default directory where the files will be downloaded to your PC, press "**ALT S**" then highlight " **FILE/PATH OPTIONS**" and press "**ENTER/RETURN**." Type "**C**" to change the default path, enter the change and then press "**ENTER/RETURN**" followed by the " **ESC**" key. To save the new def ault directory setting, highlight " **SAVE SETUP OPTIONS**," and press "**ENTER/RETURN**." Press "**ESC**" to exit setup utility.

5. Both the CARS FEP and PCPLUS will indicate that the file transfer was completed successfully or if there was an error. Upon completion, the system will return you to the MAIN MENU SCREEN.

ANNEX F - TAB 1
ACCESSING THE COMSEC AUTOMATED REPORTING SYSTEM (CARS)

CARS MAIN MENU SCREEN

acct# Abc123 **Main menu**

<C> Change password
<D> Download file
<G> Goodbye
<L> List files available
<M> Mail file
<R> Reset file
<U> Upload file
<V> View file

C,D,G,L,M,U,V: Goodbye

ALT-Z FOR HELP I VT102 I FDX I 9600 N81 I LOG CLOSED I PRINT OFF I ON -LINE

********** **USER GUIDANCE** **********

1. Selecting the " **G**" (i.e., goodbye) option allows you to log off of the CARS FEP.

2. Type "**G**" to proceed and the system will prompt you, "Are you sure?" Type "**Y**" to proceed (or " **N**" to return to the MAIN MENU) and press "**ENTER/RETURN**."

3. At this point the system will inform you, " DO NOT HANGUP!! Cleaning account ..." "Cleaning" account is the process by which the CARS FEP deletes account-specific files from your mailbox that you have already downloaded which is indicated by "download" in the "SOURCE" column on the LIST FILES SCREEN . To retain or prevent downloaded account-specific files from being deleted from your mailbox, you must execute the "R" (i.e., reset file) option (explained later). This is also when the CARS FEP sends any file that you may have uploaded using the Upload option to NKDS for processing.

4. Do **NOT** hang up your STU -III until instructed to do so by the system (i.e., only after the STU -III secure mode light goes out).

ANNEX F - TAB 1

ACCESSING THE COMSEC AUTOMATED REPORTING SYSTEM (CARS)

5. **AFTER** the secure mode light goes out , hang up your STU -III and your telephone connection to the CARS FEP will be terminated.

6. Press "**ALT X**" to end PCPLUS and exit to the DOS prompt.

LIST FILES SCREEN

FILE NAME	EXT	SIZE	CREATE DATE	SOURCE
updt0595	bbs	2971	Jun 30 12:03	COMMON
mcmsr	bbs	6844546	Jun 30 12:03	COMMON
nkds	bbs	220	Jun 30 12:03	COMMON
123456	mic	568	Jun 1 08:00	

I Hit RETURN to continue I

ALT-Z FOR HELP I VT102 I FDX I 9600 N81 I LOG CLOSED I PRINT OFF I ON -LINE

********** **USER GUIDANCE** **********

1. Selecting the "L" (i.e., list files available) option will display the names of all files in your mailbox. These files may be downloaded and/or viewed. When entering file names (including extensions), ensure that the names are entered EXACTLY as shown.

All file names must include a period as part of the extension (e.g., "bbs" would be entered as ".bbs").

2. Type "**L**" to view the list of available files.

3. The LIST FILES SCREEN provides information in five columns as follows:

a. FILE NAME : The name of the file.
b. EXT : This is extension or type of file (e.g., .mic, .inv, .chk, .bbs).
c. SIZE : The size of the file in bytes.
d. CREATE DATE : Date the file was added to your mailbox.
e. SOURCE : This is the type of file (e.g., COMMON, downloaded, or blank).

ANNEX F - TAB 1
ACCESSING THE COMSEC AUTOMATED REPORTING SYSTEM (CARS)

4. File Source information:

a. A "COMMON" source file is one that has been disseminated to ALL accounts. "Common" source files will remain on the CARS FEP until deleted by DCMS.

b. When the source column is "blank", this indicates that a file is only for your account. "Blank" source files, after they are downloaded to your PC, will automatically be deleted from your mailbox when you log off of CARS unless you elect to retain the file(s) using the file reset option.

c. "DOWNLOADED" in the source column indicates that you have downloaded the file to your PC.

d. "UPLOADED" in the source column indicates that you have uploaded the file for processing.

5. Press "**ENTER/RETURN**" to see more file names. If there are no more files to view, the system will return you to the MAIN MENU SCREEN .

MAIL SCREEN

acct # ABC123 MAIL menu

<1>	**10**	**<2>**	**20**
<3>	**30**	**<4>**	**50**
<5>	**70**	**<6>**	**80**
<7>	**90**	**<8>**	**TA1**
<9>	**TA2**	**<10>**	**TA3**

<Q> Quit to Main Menu

Enter Selection 1 - 10, Q:

ALT-Z FOR HELP I VT102 I FDX I 9600 N81 I LOG CLOSED I PRINT OFF I ON -LINE

********** **USER GUIDANCE** **********

1. Selecting the " **M**" (i.e., mail) option allows you to send E-mail to selected mailboxes at DCMS. Ensure that your E -mail is in the form of an ASCII -text file prior to commencing the upload or transfer to DCMS. PCPLUS has an online ASCII text edit program which can be used by pressing "**ALT A**."

ANNEX F - TAB 1

ACCESSING THE COMSEC AUTOMATED REPORTING SYSTEM (CARS)

2. Do **NOT** address E-mail to menu options 5 or 7 through 10 (i.e., codes 70, 90, TA1, TA2, and TA3). The remaining codes equate to the various departments at DCMS.

3. E-mail will be submitted using the following format:

a. Date: (enter the date of your E-mail).

b. From: (account number).

c. To: (enter DCMS code).

d. Subj:

e. Text: Enter the text of your E-mail.

f. POC/Tele: Enter point of contact and a telephone number.

4. Type "**M**" to proceed and enter the number corresponding to the office that you want your E-mail to go to (e.g., enter "2" to send E-mail to 20 department).

5. The system will then prompt you to enter the name of the file to be sent. Enter the filename (with extension, if applicable) and press "**ENTER/RETURN**."

6. The system will indicate that you have thirty (30) seconds to start sending. At this time you will need to invoke or commence the upload function of PCPLUS by pressing the "**page up**" key and then pressing "**Y**" (for YMODEM (batch)).

7. Next, the system will prompt you to enter the "file spec" (file spec means the DOS path and file name (i.e., C:\MEMO.TXT or A:\MEMO.TXT)) of the file that you want to forward. Enter the file spec, plus filename, and press "**ENTER/RETURN**" to start transferring the file to DCMS.

8. Upon completion of the transfer, the system will prompt you "file received" and return you to the MAIN MENU SCREEN. (**NOTE**: The files are actually in a holding queue and will be transmitted to DCMS when you execute the "**G**" or goodbye option.)

ANNEX F - TAB 1

ACCESSING THE COMSEC AUTOMATED REPORTING SYSTEM (CARS)

CARS MAIN MENU SCREEN

acct# Abc123 **CARS Main menu**

<C> Change password
<D> Download file
<G> Goodbye
<L> List files available
<M> Mail file
<R> Reset file
<U> Upload file
<V> View file

C,D,G,L,M,U,V: Reset

ALT-Z FOR HELP I VT102 I FDX I 9600 N81 I LOG CLOSED I PRINT OFF I ON -LINE

********** **USER GUIDANCE** **********

1. Selecting the " **R**" (i.e., file reset) option allows you to retain account-specific files in your mailbox that have been downloaded to your PC. By utilizing this option you prevent downloaded files (except files with source as COMMON) from being deleted from your mailbox when you log off of the CARS FEP.

2. Type "**R**" to proceed and the system will prompt you for the filename of the file to be reset. Type the name of the file (including extensions) and press "**ENTER/RETURN**."

3. Upon completion, the system will return you to the MAIN MENU SCREEN.

4. You can tell if the selected file has been reset by checking the source column on the LIST FILES SCREEN and verifying that it is no listed as " **DOWNLOADED**."

ANNEX F - TAB 1

ACCESSING THE COMSEC AUTOMATED REPORTING SYSTEM (CARS)

UPLOAD FILE SCREEN

```
acct#   Abc123              CARS Main menu
                                                +_____________________+
                           <C>  Change  password          PROTOCOL:  YMODEM  BATCH
                           <G>  Goodbye                   FILE SIZE:  2971
                           <L>  List  files  available    BLOCK CHECK:  CRC
                           <M>  Mail  file                TOTAL  BLOCKS:  3
                           <R>  Reset  file               TRANSFER  TIME:  00:08
                           <U>  Upload  file              TRANSMITTED:  100%
                           <V>  View  file                BYTE  COUNT:  3072
                                                          BLOCK  COUNT:  3
                           C,D,G,L,M,U,V:  Upload         ERROR COUNT:  0
                                                          LAST MESSAGE:  FILE RENAMED

      What is the filename?  (8 characters + extension)  cars     PROGRESS:______
      You have 30 seconds to start sending.              +_____________+

      File transfer in progress.... press  "ESC"  key to abort.
```

********** **USER GUIDANCE** **********

1. Selecting the "**U**" (i.e., upload file) option allows you to transfer ETR files from your PC to DCMS.

2. Type "**U**" to proceed and the system will prompt you for the filename of the file you want to upload. Enter the name of the file plus extension, if any, and press "**ENTER/RETURN**."

3. The system will indicate that you have thirty (30) seconds to start sending. At this time you will need to invoke or commence the upload function of PCPLUS by pressing the "**page up**" key and then pressing "**Y**" (for YMODEM (batch)).

4. Next, the system will prompt you to enter the "file spec" (file spec means the DOS path and file name (i.e., C:\123456.012 or A:\123456.012)) of the file that you want to upload. Enter the file spec and press "**ENTER/RETURN**" to start transferring the file to DCMS.

5. Both the CARS FEP and PCPLUS will indicate that the file transfer was completed successfully or if there was an error. Upon completion, the system will return you to the MAIN MENU SCREEN.

ANNEX F - TAB 1

ACCESSING THE COMSEC AUTOMATED REPORTING SYSTEM (CARS)

VIEW FILE SCREEN

(text of file selected for viewing)
xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
.....
xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

********** **USER GUIDANCE** **********

1. Selecting the " **V**" (i.e., view file) option allows you to view files in your mailbox.

2. Type "**V**" to proceed and the system will prompt you for the filename of the file to be viewed. Enter the filename (with extension) and press "**ENTER/RETURN**."

NOTE: To obtain the name of files that can be viewed, go to the LIST FILES SCREEN by selecting the " **L**" option from the MAIN MENU SCREEN .

3. If the file is so large that it extends beyond the viewable screen, use the following commands to read the entire file:

HELP Commands for "Viewing" Files on the FEP : The following keys will assist you in viewing large files on the FEP.

Key:		Function:
h	H	Display this help

PLEASE NOTE, following keys are case sensitive

q	ZZ	Exit
e	CR	Forward one line
y		Backward one line
f	SPACE	Forward one window
b		Backward one window
d		Forward one half-window
u		Backward one half-window
F		Forward forever; like "dial -f"

ANNEX F - TAB 1

ACCESSING THE COMSEC AUTOMATED REPORTING SYSTEM (CARS)

Key:	Function:
r	Repaint screen
R	Repaint screen, discarding buffered input
g p	Go to first line in file
G	Go to last line in file

NOTE: Default "window" is the screen height
Default "half-window" is half of the screen height

Command to use:	Function:
/pattern	Search forward for matching line
?pattern	Search backward for matching line

4. Once the system has displayed a file for viewing, you can also search (forward or backward) the text for a string of characters (e.g., USKAT A 12345). Type "/" to search forward or "?" to search backward followed by the string of characters you are looking for and press "**ENTER/RETURN**." (**NOTE**: The search function is case sensitive (i.e., your search string must be entered **EXACTLY** like the text you are looking for.) When the search is completed, the search command will be removed from the bottom of the screen.

5. Type "**q**" to quit and the system will return you to the MAIN MENU SCREEN.

ANNEX F - TAB 2

ACCESSING THE COMSEC AUTOMATED REPORTING SYSTEM (CARS)

CHANGING MONITOR (i.e, a CRT) WIDTH

1. To view the CMSR on line, your terminal must be set to a column width of 132 characters. Complete the following steps to change the width of your terminal:

a. After PCPLUS has been started, press "**ALT S**."

b. Highlight "**TERMINAL OPTIONS**," press "**ENTER/RETURN**."

c. Type "**L**" (for terminal width), press the space bar until "132" is displayed, and press "**ENTER/RETURN**" to save the change.

d. Press the "**ESC**" key to return to the previous menu.

e. Highlight "**DISPLAY/SOUND OPTIONS**" and press "**ENTER/RETURN**."

f. Type "**I**" (for video startup mode), press the space bar until "**USER MODE**" is displayed, and then press "**ENTER/RETURN**" to save the change.

g. Type "**K**" (for user video mode), enter "**87**", and press "**ENTER/RETURN**" to save the change.

h. Press the "**ESC**" key to return to the previous menu.

i. Highlight "**SAVE SETUP OPTIONS**" and press "**ENTER/RETURN**."

j. Press the "**ESC**" key to exit the setup menu.

k. To "visually" reset your screen width to 132, you must exit PCPLUS. Press "**ALT X**", type "**Y**" to exit to DOS, then restart PCPLUS from the DOS prompt by typing "PCPLUS" and pressing "**ENTER/RETURN**." At this time, your monitor width will be set to "132" vice "80."

2. To return your monitor width to 80, follow the above procedures by substituting "80" in place of "132" and "0" in place of "87."

ANNEX H

CMS ACCOUNT ESTABLISHMENT REQUEST (R

R 071830Z JUN 93 ZYB
FM USS RANGER
TO DCMS WASHINGTON DC//30//
INFO CINCPACFLT PEARL HARBOR HI//N5//
COMNAVAIRPAC SAN DIEGO CA//N321//
CMIO NORFOLK VA//20//
DIRNSA FT GEORGE G MEADE MD//Y111//
NISEEAST DET NORFOLK VA//526CS/635SB//
NISEEAST CHARLESTON SC//40C//
UNCLAS//N02280//
MSGID/GENADMIN/RANGER//
SUBJ/CMS ACCOUNT ESTABLISHMENT//
REF/A/DOC/DCMS/01SEP92//
REF/B/LTR/COMNAVAIRPAC N321/1MAY93//
REF/C/DOC/CLF/CPF/CINCUSNAVEURINST C2282.1/1NOV91//
REF/D/RMG/DIRNSA/050403ZJUN93//
NARR/REF A IS CMS POLICY AND PROCEDURES MANUAL. REF B PROVIDES CERTIFICATION AUTHORIZATION TO STORE CLASSIFIED/COMSEC MATERIAL AND AUTHORIZES CMS ACCOUNT ESTABLISHMENT. REF C CONTAINS AUTHORIZED KEYING MATERIAL ALLOWANCE FOR PACFLT SHIPS. REF D IS CONTROLLING AUTHORITY VALIDATION.//
POC/SAILOR/CTOCS/DSN 123 -4567//
RMKS/1. REQUEST ESTABLISHMENT OF A CMS ACCOUNT TO SUPPORT OPERATIONAL REQUIREMENTS. FOLLOWING INFORMATION PROVIDED IAW ARTICLE 405 AND ANNEX H OF REF A:
A. COMMAND TITLE : USS RANGER (CV -61)
B. MAILING ADDRESS : USS RANGER (CV -61)
COMM DEPT
FPO AP 96631
C. ISIC AND VALIDATION REF : COMNAVAIRPAC; REF B GERMANE.
D. HCI: TOP SECRET.
E. COMMAND MEETS STORAGE/PHYSICAL SECURITY REQUIREMENTS FOR STORING TOP SECRET MATERIAL AS VALIDATED BY REF B.
2. REQUIRED MATERIAL :
A. KEYING MATERIAL (READ SHORT TITLE/QTY):
(1) USKAT 11111/ONE
(2) USKMT 11112/ONE
(3) ALL KEYMAT FOR CV'S LISTED IN REF C.

ANNEX H

CMS ACCOUNT ESTABLISHMENT REQUEST (R

B. MANUALS/EQUIP/RELATED DEVICES (READ SHORT TITLE/QTY):
(1) KAM -222/ONE
(2) KAO -222/ONE
(3) KYX -11/TWO
(4) KG -11/ONE
C. VALIDATION AUTHORITY/JUSTIFICATION : REF D GERMANE.
3. DMR: 930724
A. DURATION : TEMPORARY 930724 -930820
B. SHIPPING INSTRUCTIONS : MTL WILL BE PICKED UP AT CMIO NORFOLK.//

ANNEX H

CMS ACCOUNT ESTABLISHMENT REQUEST (R

1. **Purpose**: A request to establish a CMS account is to be submitted only when it is not possible to draw needed materials from an existing CMS account (either within the organization or located in close proximity thereto). The request will be submitted after appointment of a qualified CMS Custodian and Alternate(s) and fulfillment of the requirements in paragraph 2 below.

2. **ISIC requirements**: A command's ISIC must perform the following prior to a subordinate command submitting a request to establish a CMS account:

a. Validate requirement for the CMS account.

b. Validate command compliance with the minimum physical security requirements for safeguarding COMSEC material. (**NOTE**: Chapter 5 contains physical security requirements.)

c. Determine the required COMSEC mate rial based on command mission and communications capabilities.

d. Obtain CA authorization for COMSEC material not listed in a standard allowance instruction (e.g., for USN afloat units - CLF/CPF/CINCUSNAVEURINST C2282.1 (series)).

3. **Lead time**: A minimum of 45 days is required to establish a CMS account and to provide the initial COMSEC material.

4. **Submission**: A letter or message must be forwarded to the appropriate addressees listed in Article 405.d. All correspondence for DCMS must contain the office code //30//.

5. **Preparation guidance**: The following information must be provided in the account establishment request:

a. Command title, mailing address, ISIC, HCI, ISIC authorization to establish the account and validation that the command meets (R physical security requirements for storing COMSEC material.

b. List of required COMSEC material by short title and quantity.

ANNEX H

CMS ACCOUNT ESTABLISHMENT REQUEST

c. Controlling authority validation. (**NOTE**: Not required when material is listed in a standard allowance instruction (e.g., CLF/CPF/CINCUSNAVEURINST C2282.1 (series).)

d. Period material is required (permanent or temporary). (**NOTE**: Specify exact dates only for that material required on a temporary basis.)

e. Specify date material required (DMR) at the command.

f. Shipping instructions. (**NOTE**: Identify DCS station or provide alternative shipping instructions (e.g., material will be picked up from CMIO Norfolk). (R

6. **Delivery of material**: After submitting a request to establish a CMS account, the requesting command must:

a. Coordinate with the area DCS station and establish a DCS account.

b. Submit a CMS Form 1 to CMIO Norfolk **ONLY** if the command will be picking up material from the CMIO. (**NOTE**: Annex I contain instructions for submitting a CMS Form 1.) (R

ANNEX I
CMS FORM 1

_____
(DDMMYY)

From: _____
_____
(Command title and mailing address)

To: **CMIO** Norfolk

Subj: **AUTHORIZATION TO RECEIPT FOR AND COURIER COMSEC MATERIAL**

Ref: (a) CMS 1, Article 405

1. In accordance with reference (a), the below named individuals are authorized to receipt for and courier COMSEC material for the above CMS account command:

RATE/RANK NAME (Last,First,MI)	**SSN**	**SECURITY CLEARANCE**	**POSITION**	**SIGNATURE**
GRADE				

---LAST ENTRY---

2. a. **CMS Account number:** _____
   b. **Highest Classification Indicator (HCI):**_____
   c. **Command Telephone number(s):** **COMM: ( )**_____
      DSN: _____
   d. **ISIC:** _____

3. I certify that the individuals identified above are assigned to my command; are authorized to receive and courier COMSEC material for the above command/CMS account; and possess a security clearance equal to or higher than that of the COMSEC material being handled.

AUTHORIZING OFFICIAL SIGNATURE: _____

RANK/GRADE	**NAME (Last, first, MI)**	**POSITION (e.g., CO, OIC)**

(CMS Form 1)

ANNEX I
CMS FORM 1

1. Purpose: CMS Form 1 is a locally prepared form that is used to authorize appropriately cleared personnel, one of whom must be the CMS Custodian or Alternate, to receipt for and courier COMSEC material between their command and CMIO. CMS Form 1 must be submitted on command letterhead (less messages). (**NOTE**: ANCRS-generated CMS 1 Forms are acceptable.) (R

NOTE: CMS Form 1 is required **ONLY** if material will be picked up from CMIO. (R

2. Preparation: All information, less signatures, must be typed or printed (in black ink); signatures must be signed on both copies of CMS Form 1 in black ink.

a. **Date**: Enter the date the authorizing official signs the form.

b. **Command title and address**: Enter the command name and complete mailing address.

c. **Authorized personnel**: Enter the required information and have each individual verify the information by affixing their signature. Enter "LAST ENTRY," immediately below the last name.

d. **CMS account number, HCI, telephone numbers, and ISIC**: Enter the required information.

e. **Authorizing official signature and data**: The authorizing official must be the CO, OIC, or SCMSRO of the CMS account command or the designated individual acting on their behalf.

3. Submission: The CMS Form 1 must be submitted via letter or facsimile. In the event of a short-fused emergent operational requirement, a message containing the same information as a CMS Form 1 may be submitted in order to receipt for and courier COMSEC material. Use of a message does not negate the requirement for an account to ensure that CMIO holds a valid CMS Form 1. (R

4. Disposition: Forward the original copy of CMS Form 1 to CMIO and retain the second copy in the CMS Chronological File. (R

5. Changes: Whenever there is a change in the authorizing official or the personnel authorized to receipt for and courier COMSEC material, a new CMS Form 1 must be submitted.

6. CMIO Action: Retain CMS Form 1 on file for each CMS account. Ensure that COMSEC material is received from/released only to personnel that are listed on a valid CMS Form 1.

ANNEX J

SAMPLE CMS/LH ACCOUNT
LETTER/MEMORANDUM OF APPOINTMENT (LOA/MOA)

_____
(DDMMYY)

From: Commanding Officer
To: (Rank/Rate /Grade, Name, and SSN)

Subj: **LETTER/MEMORANDUM OF APPOINTMENT**

Ref: (a) CMS -1

1. In accordance with reference (a), you are hereby appointed as (CMS Custodian, Alternate CMS Custodian, LH CMS Custodian or Alternate LH CMS Custodian, or CMS Clerk) for this command.

2. **CMS account number:** _____.

3. CMS COI (A -4C -0014 or A-4C-0031) completed on (YYMMDD) at (name/location of CMS COI).

4. **Security clearance:** (Top Secret/Secret, etc., as applicable).

5. Following designation requirements contained in (Article 415 or 420, as applicable) of reference (a) are waived:

a. _____
b. _____
(identify authority for and specific requirement(s) waived; if no requirements waived, indicate "N/A")

(Signature of Commanding Officer)

NOTE: 1. Retain the original copy of the LOA/MOA in the Correspondence/Message File for two years from the date an individual has been relieved of his/her duties.

2. LH accounts must forward the original copy of LOA/MOAs to the CMS account command and retain a copy in the LH Correspondence/Message File.

3. Do **not** forward individual LOA/MOAs to DCMS.

ANNEX K
CMS RESPONSIBILITY ACKNOWLEDGMENT FORM

From: _____
(Rank/Rate, Full Name, SSN, and Command of CMS User)

To: **(CMS Custodian or LH Custodian)**, _____
(Name of Command)

Subj: **CMS RESPONSIBILITY ACKNOWLEDGMENT**

Ref: (a) (CMS 1 and/or the local command instruction governing the handling, accountability, and disposition of COMSEC material)

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

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

3. I have r eceived a copy of reference (a) from the (CMS Custodian or LH Custodian). If at any time I am in doubt as to the proper handling of COMSEC material that I am responsible for, I will immediately contact the (CMS or LH Custodian) and request advice.

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

SIGNATURE: _____

DATE: _____

NOTE:

ANNEX L

SAMPLE OF A LETTER OF AGREEMENT (LOA)

When the CO of a LH account or user is different from the CO of the parent account (numbered account providing COMSEC material support), a Letter or Memorandum of Agreement (LOA/MOA) is required between the two commands. This **sample** letter outlines the minimum issues to be addressed; it may, of course, be modified to include additional requirements or guidance as desired by the numbered account command.

From: Commanding Officer (numbered account command)
To: Commanding Officer (LH command or user)

Subj: COMSEC MATERIAL LETTER OF AGREEMENT

Ref: (a) (cit e letter request for material support)
(b) CMS -1

Encl: (1) (cite locally prepared CMS instruction(s))

1. In response to reference (a), this command agrees to provide COMSEC material support to your command with the following provisions:

a. **Compliance with Enclosure (1)**: (LH command/user) will ensure that all personnel authorized to handle and use the COMSEC materials provided by this command comply with the guidance of enclosure (1). To this end, (LH command/user) will conduct training sessions at regular intervals on the proper handling, accounting, use and safeguarding of COMSEC materials. Particular emphasis must be given to educating personnel in how to identify COMSEC incidents and Practices Dangerous to Security (PDS).

b. **Reporting of COMSEC Incidents**: In the event of a COMSEC incident, LH Custodian/user will report the incident to the addressees outlined in reference (b) and will include this command as an information addressee on the initial report and any amplifying reports.

OR

Reporting of COMSEC Incidents: In the event of a COMSEC incident, LH Custodian/user will report the incident immediately to this command and the LH/User CO. The information provided must be of sufficient detail to enable this command to assume responsibility for reporting the incident.

ANNEX L

SAMPLE OF A LETTER OF AGREEMENT (LOA)

c. **Responsibility for Certifying Clearances/Access**: The LH command/user will accept 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. The LH command/user will also require personnel who are issued COMSEC material to complete a CMS Responsibility Acknowledgment Form (see Annex K).

d. **Notification of Custodian Appointments**: This command will be notified of new LH Custodian appointments and changes in custodian positions held. This notification will consist of forwarding the original copy of the Letter/Memorandum of Appointment as contained in Annex J of CMS 1. This command will also be notified, in writing, when a Custodian has been relieved of his/her duties.

e. **Storage/Facility Clearance**: (LH command/user) will provide this command with written certification that the safe and/or vault of the LH Custodian/user is approved for storage of the highest classification of COMSEC material to be stored.

ANNEX M

EMERGENCY PROTECTION OF COMSEC MATERIAL

1. Purpose: This annex prescribes policy and procedures for planning, protecting, and destroying COMSEC material during emergency conditions.

2. Emergency Protection Planning:

a. Every command that holds classified COMSEC **or** CCI material must prepare emergency plans for safeguarding such material in the event of an emergency.

b. For commands located within the continental United Station (CONUS), planning need consider only natural disasters (e.g., fire, flood, tornado, and earthquake).

c. For commands located outside of CONUS, planning must consider both natural disasters **and** hostile actions (e.g., enemy attack, mob action, or civil uprising).

d. For natural disasters, planning should be directed toward maintaining security control over the material until order is restored.

e. Planning for hostile actions must concentrate on the safe evacuation or secure destruction of the COMSEC material.

f. These plans will be incorporated into the overall Emergency Action Plan (EAP) of the command.

g. Efficient planning and training which involves every individual who uses COMSEC material increases the probability of preventing its loss or compromise during an emergency.

h. The operating routines for COMSEC facilities should be structured so as to minimize the number and complexity of actions which must be taken during emergencies to protect COMSEC material.

i. The command EAP/EDP, if not specific to LH/User operations, must be modified or annexed to include specific actions to be taken by LH/User accounts.

j. Any detachment which operates independently (i.e., (A aircraft and communications/special purpose vans) from their parent command should have their own unique EAP/EDP specifically tailored for those times of independent operation. In all cases, they should be included in the command's EAP/EDP."

ANNEX M

EMERGENCY PROTECTION OF COMSEC MATERIAL

3. Guidelines For Minimizing Actions:

a. Hold only the minimum amount of COMSEC material at any time (i.e., routine destruction should be conducted frequently and excess COMSEC material disposed of as directed by appropriate authorities).

b. Store COMSE C material to facilitate emergency removal or destruction (e.g., separate COMSEC material from other classified material, and segregate COMSEC keying material by status, type and classification).

NOTE: COMSEC material which has been designated for "NATO" use is not exclusively NATO material but is in fact COMSEC material. Consequently, this material need not be separated from other COMSEC material but must be stored and segregated by status and classification.

c. As emergency situations develop, initiate precautionary destruction or evacuation of all material not immediately needed for continued operational effectiveness. After destroying material, notify appropriate authorities so they may begin resupply planning.

4. Preparedness Planning For Disasters: Planning for disasters must provide for:

a. Fire reporting and initial fire fighting by assigned personnel.

b. Assignment of on-the-scene responsibility for ensuring protection of the COMSEC material held.

c. Security or removing classified COMSEC material and evacuating the area(s).

d. Protection of material when admission of outside fire fighters into the secure area(s) is necessary.

e. Assessment and reporting of probable exposure of classified COMSEC material to unauthorized persons during the emergency.

f. Post-emergency inventory of classified COMSEC and CCI material and reporting any losses or unauthorized exposure to appropriate authorities.

ANNEX M
EMERGENCY PROTECTION OF COMSEC MATERIAL

5. Preparedness Planning for Hostile Actions: Planning for hostile actions must take into account the possible types of situations which may occur (e.g., an ordered withdrawal over a specified period of time, a hostile environment situation where destruction must be carried out in a discrete manner to avoid triggering hostile actions, or fully hostile imminent overrun situations.) Ensure that the plan provides for the following:

a. Assessing the threat of occurrence of the various types of hostile emergencies at the particular activity and of the threat that these potential emergencies pose to the COMSEC material held.

b. The availability and adequacy of physical security protection capabilities (e.g., perimeter controls, guard forces, and physical defenses) at the individual buildings and other locations when COMSEC material is held.

c. Facilities for effecting emergency evacuation of COMSEC material under emergency conditions, including an assessment of the probable risks associated with evacuation.

NOTE: Except under extraordinary conditions (e.g., an urgent need to restore secure communications after relocation), COMSEC keying material should be destroyed rather than evacuated.

d. Facilities and procedures for effecting secure emergency destruction of COMSEC material must address:

(1) Adequate number of destruction devices,

(2) Availability of electrical power,

(3) Secure storage facilities nearby,

(4) Adequately protected destruction areas,

(5) Personnel assignments, and

(6) Clear delineation of responsibilities for implementing emergency destruction.

e. Precautionary destruction of COMSEC material, particularly maintenance manuals (KAMs) and keying material which is not operationally required to ensure continuity of operations during the emergency.

(1) In a deteriorating situation all "full" maintenance manuals (i.e., those containing cryptographic logic information) which are not absolutely essential to continued mission accomplishment must be destroyed.

ANNEX M

EMERGENCY PROTECTION OF COMSEC MATERIAL

(2) When there is insufficient time under emergency conditions to completely destroy such manuals, every reasonable effort must be made to remove and destroy their sensitive pages (i.e., those containing cryptographic logic/classified schematics).

NOTE: 1. Sensitive pages in U.S. -produced KAMs are listed on fold-out Lists of Effective Pages at the rear of other textual portions.
2. Some KAMs further identify their sensitive pages by means of gray or black diagonal or rectangular markings at the upper portion of the binding edge.

(a) To prepare for possible emergency destruction of sensitive pages from KAMs in areas or situations where capture by hostile forces is possible, comply with the following guidance:

1 Apply distinctive markings (e.g., red stripes) to the binder edge and covers of all KAMs containing identified sensitive pages.

2 Remove the screw posts or binder rings, or open the multi -ring binder, whichever is applicable.

3 Remove each sensitive page from the KAM and cut off the upper left -hand corner of the page so that the first binder hole is removed. Care must be taken not to delete any text or diagram.

(b) Should it become necessary to implement emergency destruction, the sensitive KAM pages may be removed as follows:

1 Remove the screw posts or binder rings, or open the multi -ring binder and remove all p ages from the KAM.

2 Insert a thin metal rod (e.g., wire or screwdriver) through the remaining top left -hand hole of the document.

3 Grasp the rod in both hands and shake the document vigorously; the sensitive pages should fall out freely.

f. Establishment of emergency communications procedures.

(1) External communications during emergency situations should be limited to contact with a single remote point.

(2) This point will act as a distribution center for outgoing message traffic and a filter for incoming queries and guidance.

(3) When there is warning of hostile intent and physical security protection is inadequate to prevent overrun of the facility, secure communications should be discontinued in time to allow for thorough destruction of all classified COMSEC and CCI material, including classified and CCI elements of COMSEC equipment.

6. Preparing The Emergency Plan:

a. The emergency plan shoul d be prepared by the person most aware of the extent and significance of the COMSEC material on hand.

b. The Commanding Officer or other responsible official must be aware of and approve the emergency plan.

c. If the plan calls for destroying COMSEC material, all destruction material, devices, and facilities must be readily available and in good working order.

d. The plan must be realistic; it must be workable, and it must accomplish the goals for which it is prepared. Factors which will contribute to this are:

(1) All duties under the plan must be clearly and concisely described.

(2) All authorized personnel at the command should be aware of the existence of the plan.

(a) Each individual assigned duties assigned under the plan must receive detailed instructions on how to carry out those duties when the plan is implemented.

(b) All personnel should be familiar with all duties so that changes in assignment may be made, if necessary. This may be accomplished by periodically rotating the emergency duties of all personnel.

(3) Training exercises should be conducted annually (quarterly exercises are recommended) to ensure that everyone, especially newly assigned personnel who might have to take part in an actual emergency, will be able to carry out their duties.

NOTE: If necessary, the plan should be modified based on the training exercise results.

ANNEX M

EMERGENCY PROTECTION OF COMSEC MATERIAL

(4) The three options available in an e mergency are securing the material, removing it from the scene of the emergency, or destroying it. Planners must consider which of these options may be applicable to their command.

(5) For example, if it appears that a civil uprising is to be short lived, and the COMSEC facility is to be only temporarily abandoned, the actions to take could be:

(a) Ensure that all superseded keying material has been destroyed.

(b) Gather up the current and future keying material and take it along.

(c) Remove classified and CCI elements from crypto -equipment and lock them, along with other classified COMSEC material, in approved storage containers.

(d) Secure the facility door(s), and leave.

(e) Upon return, conduct a complete inventory.

NOTE: If it appears that the facility is likely to be overrun, the emergency destruction plan should be put into effect.

7. Emergency Destruction Planning: Three categories of COMSEC material which may require destruction in hostile emergencies are COMSEC keying material, COMSEC -related material (e.g., maintenance manuals, operating instructions, and general doctrinal publications), and equipment.

a. **Precautionary Destruction:** When precautionary destruction is necessary, destroy keying material and non -essential manuals in accordance with this Annex and your EAP.

b. **Complete Destruction:** When sufficient personnel and facilities are available, assign different persons to destroy the material in each category by means of separate destruction facilities and follow the priorities listed herein as incorporated into your EAP.

NOTE: When personnel and/or destruction facilities are limited, join the three categories and destroy the material following the priorities listed in Priority List C.

ANNEX M

EMERGENCY PROTECTION OF COMSEC MATERIAL

8. Emergency Destruction Priorities:

a. **Precautionary Destruction Priority List A:**

(1) Superseded keying material and secondary variables.

(a) TOP SECRET p rimary keying material.
(b) SECRET, CONFIDENTIAL, and Unclassified primary keying material.

(2) Future (reserve on board) keying material for use one or two months in the future.

(3) Non-essential classified manuals:

(a) Maintenance manuals.
(b) Operating manuals.
(c) Administrative manuals.

b. **Complete Destruction Priority List B:** When sufficient personnel and facilities are available, destroy COMSEC material in the following order:

(1) Keying Material:

(a) All superseded keying material designated CRYPTO, except tactical operations and authentication codes classified below SECRET.

(b) Currently effective keying material designated CRYPTO (including key stored electrically in crypto equipment and FDs), except unused two -holder keying material and unused one -time pads.

(c) TOP SECRET multiholder (i.e., more than two holders) keying material marked CRYPTO which will become effective within the next 30 days.

(d) Superseded tactical operations codes classified below SECRET.

(e) SECRET and CONFIDENTIAL multiholder keying material marked CRYPTO which will become effective within the next 30 days.

(f) All remaining classified keying material, authentication systems, maintenance, and unused one -time pads.

ANNEX M

EMERGENCY PROTECTION OF COMSEC MATERIAL

(2) **COMSEC Aids:**

(a) Complete COMSEC equipment maintenance manuals or their sensitive pages. When there is insufficient time to completely destroy these manuals, every reasonable effort must be made to destroy their sensitive pages.

(b) National, department, agency, and service general doctrinal guidance publications.

(c) Status documents showing the effective dates for COMSEC keying material.

(d) Keying material holder lists and directories.

(e) Remaining classified pages of maintenance manuals.

(f) Classified cryptographic and non -cryptographic operational general publications (e.g., AMSGs and NAGs).

(g) Cryptogra phic Operating Instructions (KAOs).

(h) Remaining classified COMSEC documents.

(3) **Equipment:** Make a reasonable effort to evacuate equipment, but the immediate goal is to render them unusable and unrepairable.

NOTE: Although it is desirable to destroy jeopardized crypto -equipment so thoroughly that logic reconstruction is impossible, this cannot be guaranteed in most field environments.

(a) Zeroize the equipment if the keying element (e.g., key card, permuter plug) cannot be physically withdrawn.

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

(c) Destroy remaining classified elements. (**NOTE:** Unclassified chassis and unclassified elements need not be destroyed.)

c. **Complete Destruction Priority List C:** In cases where personnel and/or facilities are limited, follow the destruction priority list below:

ANNEX M

EMERGENCY PROTECTION OF COMSEC MATERIAL

(1) All supe rseded and currently effective keying material marked CRYPTO (including key stored electrically in crypto -equipment and fill devices), except tactical operations codes and authentication systems classified below SECRET, unused two -holder keying material, and unused one -time pads.

(2) Superseded tactical operations codes classified below SECRET.

(3) Complete COMSEC equipment maintenance manuals or their sensitive pages.

(4) Classified general COMSEC doctrinal guidance publications.

(5) Cl assified elements of COMSEC equipment.

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

(7) Remaining classified COMSEC material.

(8) Future editions of multiholder (i.e., more than two holders) keying material and current but unused copies of two -holder keying material.

9. Conducting Emergency Destruction: Any of the methods approved for routine destruction of classified COMSEC material may be used for emergency destruction.

a. **Printed Matter:**

(1) Destroy keying material and other classified COMSEC publications beyond reconstruction.

(2) Destroy all "full" maintenance manuals (i.e., those containing cryptographic logic information/classified schematics). When time does not permit, every reasonable effort must be made to remove and destroy their sensitive pages in accordance with paragraph 5.e.

b. **Classified Crypto-Equipment:** Render classified crypto-equipment inoperable (i.e., beyond reuse).

(1) If time permits, destroy the cryp tographic logic of the equipment beyond reconstruction by removing and destroying the classified portions of the equipment, which include certain printed circuit boards and multi -layer boards, and keyed permuting devices.

ANNEX M

EMERGENCY PROTECTION OF COMSEC MATERIAL

(2) If these classified elements are destroyed, it is not necessary to destroy the remainder of the equipment.

c. **Emergency Destruction in Aircraft:** When time or facility limitations preclude complete destruction of COMSEC material aboard aircraft, make all reasonable efforts to prevent the material from falling into unauthorized hands.

(1) When the aircraft is operating over water and an emergency or forced landing is imminent, zeroize the COMSEC equipment and shred or tear up the keying material and disperse it. If feasible, remove the classified elements from the equipment and smash and disperse them.

(2) If an aircraft is in danger of making an emergency landing in friendly territory, zeroize the equipment and keep all the COMSEC materials in the aircraft.

(3) If the aircraft is being forced or shot down over hostile territory, first zeroize the equipment, then shred or tear up and disperse the keying material, and make all reasonable efforts to remove, smash, and disperse the classified equipment components.

d. **Emergency Destruction Aboard Ship**:

(1) If the ship is in imminent danger of sinking in a U.S.-controlled area, zeroize the equipment, destroy all COMSEC material as completely as possible in the time available, lock it in security containers and permit it to sink with the ship.

(2) If the ship is in imminent danger of capture or of sinking in an area where foreign elements would have salvage opportunities, destroy all COMSEC equipment and all keying material.

(a) Destroy all COMSEC equipment as completely as time permits, and jettison the undestroyed or partially destroyed COMSEC material overboard.

(b) Place paper items and other material that could float in weighted canvas bags before jettisoning.

10. Reporting Emergency Destruction:

a. Accurate information relative to the extent of an emergency is absolutely essential to the effective evaluation of the COMSEC impact of the occurrence, and is second in importance only to the conduct of thorough destruction.

ANNEX M

EMERGENCY PROTECTION OF COMSEC MATERIAL

b. The Commanding Officer/OIC or official responsible for safeguarding COMSEC material which has been subjected to emergency destruction, is responsible for reporting the attendant facts to the appropriate seniors in the chain of command by the most expeditious means available.

(1) **Reporting Instructions:** The senior official shall report the facts surrounding the destruction to CNO//N652//, DCMS//20//, DIRNSA//X71A//, and both operational and administrative command echelons as soon as possible; if feasible, use a secure means of reporting.

(2) **Required Information:** State in the report the material destroyed, the 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).

NOTE: If feasible, follow the reporting procedures for COMSEC Incidents as outlined in Chapter 9 of this manual. Ensure the EAP includes guidance for providing the required information.

ANNEX N

CONSTRUCTION SPECIFICATIONS FOR STORAGE VAULTS

1. **Purpose:**

a. To provide minimum standards for the construction of vaults used as storage facilities for COMSEC keying material.

b. The specifications included in this annex are not prescriptive because there are other construction techniques which will provide equivalent protection, and which may be required to meet certain operational requirements.

2. **Class "A" Vault Construction Specifications:**

a. Floors: Floors should be of poured, reinforced concrete which has a minimum thickness of eight inches and shall be reinforced with reinforcing rods.

NOTE: Reinforcing rods must be at least 3/8 inch in diameter, mounted vertically and horizontally on center not less than two inches and not greater than ten inches.

b. Walls: Walls should be of poured, reinforced concrete which has a minimum thickness of eight inches. The walls shall connect solidly with the vault roof and floor.

(1) Walls shall be reinforced with reinforcing rods, at least 3/8 inch in diameter.

(2) Reinforcing rods shall be mounted vertically and horizontally on center not less than two inches and not greater than ten inches.

c. Roof: The roof should be a monolithic reinforced concrete slab of a thickness to be determined by structural requirements, but not less than the walls and floors.

d. Ceiling: Where the existing floor-to-ceiling distance exceeds 12 feet, a vault roof, structurally equal to the vault walls, may be constructed at a height determined by structural limitations, size of equipment to be enclosed, optimum utilization of existing enclosed air space, and specific use requirements.

ANNEX N

CONSTRUCTION SPECIFICATIONS FOR STORAGE VAULTS

NOTE: Where the existing roof does not conform to the vault roof requirements stated above, a vault roof, which is structurally equal to the vault walls shall be constructed.

e. Vault Door and Frame Unit: The vault door and frame shall afford protection not less than that provided by a Class 5 vault door specified in GSA (R Federal Specification AA-D-00600 (GSA-FSS), Door, Vault, Security.

f. Lock: The combination lock shall conform to the Underwriters' Laboratories, Inc., standard No. 768, for Group 1R or Group 1. The specific lock model used shall bear a valid UL Group 1R or Group 1 label.

NOTE: All vault doors procured after the effective date of this publication must be equipped with a GSA approved combination lock that meets the requirements of Federal Specifications FF-L-2740.

3. **Class "B" Vault Construction Specifications**:

a. Floors: Floors should be of monolithic concrete construction of the thickness of adjacent concrete floor construction but not less than six inches thick.

b. Walls: Walls should be of brick, concrete block, or other masonry units and not less than eight inches thick.

(1) Hollow masonry units shall be the vertical cell type (load bearing) filled with concrete and steel reinforcement bars.

(2) Monolithic steel-reinforced concrete walls at least six inches thick may also be used, and shall be used in seismic areas.

c. Roof: The roof should be a monolithic reinforced concrete slab of not less than six inches in thickness.

d. Ceiling: The provisions of paragraph 2. d. apply.

e. Vault Door and Frame Unit: Paragraph 2. e. applies.

f. Lock: Paragraph 2. f. and the NOTE that follows it (for new vault doors) applies.

ANNEX N

CONSTRUCTION SPECIFICATIONS FOR STORAGE VAULTS

4. **Day Gate:**

ANNEX N

CONSTRUCTION SPECIFICATIONS FOR STORAGE VAULTS

b. Emergency escape device:

(1) If an emergency escape device is considered necessary, it shall be permanently attached to the inside of the door and shall not be activated by the exterior locking device or otherwise accessible from the outside.

(2) The device shall be designed and installed so that drilling and rapping the door from the outside will not give access to the vault by activating the escape device.

(3) The device shall meet the requirements of paragraph 3.3.9 of GSA Federal Specification AA-D-00600 (GSA-FSS), concerning an exterior attack on (R
the door.

c. Ventilation: If an emergency escape device is not provided, the following approved Underwriters Laboratories (UL), Inc., devices must be installed in each vault:

(1) A UL Bank Vault Emergency Ventilator.

(2) At least one UL approved fire extinguisher situated in a position near the vault door.

NOTE: These provisions are recommended even if an emergency escape device is provided.

ANNEX O
CONSTRUCTION SPECIFICATIONS FOR FIXED COMSEC FACILITIES

1. Purpose: To prescribe minimum construction requirements for fixed COMSEC facilities.

2. Construction Requirements: A fixed COMSEC facility must be constructed of solid, strong materials that will deter and detect unauthorized penetration. It must provide adequate attenuation of internal sounds that would divulge classified information through walls, doors, windows, ceilings, air vents, and ducts.

3. Walls, Floors, and Ceilings: Walls, floors, and ceilings shall be of sufficient structural strength to prevent or reveal any attempts at unauthorized penetration.

a. Walls shall be constructed from true floo r to true ceiling.

b. Ceilings shall ideally be at least as thick as the outer walls and offer the same level of security as the outer walls.

c. Where false ceilings are used, additional safeguards will be required to resist unauthorized entry (e.g., installation of an approved intrusion detection system (IDS) in the area above the false ceiling).

4. Doors and Entrance Areas: Only one door shall be used for regular entrance to the facility. Other doors may exist for emergency exit and for entry or removal of bulky items.

a. All doors shall remain closed during facility operations and should only be opened to admit authorized personnel or material.

b. The following standards apply to facility doors and entrance areas:

(1) Main entrance door:

(a)

ANNEX O

CONSTRUCTION SPECIFICATIONS FOR FIXED COMSEC FACILITIES

Metal-clad or solid hardwood doors with a minimum thickness of 1-3/4 inch.

(b) The door frame must be securely attached to the facility and must be fitted with a heavy-duty/high security strike plate and hinges installed with screws long enough to resist removal by prying.

(c) The door shall be installed to resist the removal of hinge pins. This can be accomplished by either installing the door so that the hinge pins are located inside the facility or by set screwing/welding the pins in place.

(2) Door lock: The main entrance door to facilities which are not continuously manned must be equipped with a GSA-approved, built-in Group 1-R lock.

(a) For facilities which are continuously manned, a built-in lock is not required; however, the door must be designed so that a GSA-approved Group 1-R lock can be affixed to the outside should it ever become necessary to lock the facility (e.g., in case of emergency evacuation).

(b) An electronically activated lock (e.g., cipher lock or keyless push-button lock) may be used on the entrance door to facilitate the admittance of authorized personnel when the facility is operationally manned. However, these locks do not afford the required degree of protection and may not be used to secure the facility when it is not manned.

(3) Other doors: Other doors (e.g., emergency exit doors and doors to loading docks) must meet the same installation requirements as the main facility entrance doors and must be designed so that they can only be opened from inside the facility.

NOTE: Approved panic hardware and locking devices (lock bars, dead bolts, knobs, or handles) may be placed only on the interior surfaces of other doors to the facility.

(4) Entrance areas: The facility entrance area shall be equipped with a device which affords personnel desiring admittance the ability to notify personnel within the facility of their presence.

(a) A method shall be employed to establish positive visual identification of a visitor before entrance is granted.

ANNEX O

CONSTRUCTION SPECIFICATIONS FOR FIXED COMSEC FACILITIES

(b) The entrance area shall be designed in such a manner that an individual cannot observe classified activities until cleared for access into the restricted spaces.

5. Windows: COMSEC facilities should not normally contain windows. Where windows exist, they shall be secured in a permanent manner to prevent them from being opened.

a. Windows shall be alarmed and/or barred to prevent their use as an access point.

b. Observation of internal operations of the facility shall be denied to outside viewing by covering the windows from the inside or otherwise screening the secure area from external viewing.

6. Other openings: Air vents, ducts, or any similar openings which breach the walls, floor, or ceiling of the facility shall be appropriately secured to prevent penetration.

a. Openings which are less then 90 square inches shall have approved baffles installed to prevent an audio or acoustical hazard.

b. If the opening exceeds 90 square inches, acoustical baffles shall be supplemented by either hardened steel bars or an approved intrusion detection system (IDS).

ANNEX P
"SPECIAL" PHYSICAL SECURITY SAFEGUARDS FOR DoD BLACK BULK FACILITIES

1. Purpose:

a. To delineate the physical security safeguards which are unique to those facilities operated by or for the DoD, and employ classified crypto -equipment to protect multichannel trunks passing encrypted or unclassified information, and otherwise referred to as DoD black bulk facilities.

b. The area within a structure occupied by a DoD Black Bulk facility is referred to as a "space," and it is this "space" that requires the safeguards prescribed in this Annex.

NOTE: The structure which contains the space is referred to as a "site."

2. Construction Requirements:

a. Walls: At sites which are not continuously manned, walls shall be of solid construction from true floor to true ceiling and shall be constructed in such a manner that attempts at unauthorized penetration will be detected or prevented.

b. Doors: At sites which are not continuously manned, the entrance door shall be of substantial material, (e.g., metal clad or solid wood with a minimum thickness of 1 -3/4 -inch), hinged from inside, fitted with a GSA -approved Group 1 -R lock having a dead -bolt extension, or a heavy -duty hasp and GSA-approved padlock.

(1) Other doors shall be secured from the inside.

(2) At continuously manned sites, doors need only have sufficient strength to prevent undetected forced entry.

c. Windows: At sites which are not continuously manned, all windows shall be locked from the inside and covered to prevent observation of internal operations. Additionally, at "F" sites (see paragraph 3) which are not continuously manned, windows on ground floors, basement levels, in vans, or shelters shall be securely barred or sealed.

d. Intrusion Detection System (IDS): At sites which are not continuously manned, an approved IDS shall be used on all accesses. The IDS shall be monitored at a location from which a guard(s) can be dispatched. Either U.S. or Allied personnel may be assigned to monitor the IDS and to direct the responding guard(s).

ANNEX P

"SPECIAL" PHYSICAL SECURITY SAFEGUARDS FOR DoD BLACK BULK FACILITIES

3. Categories of DoD Black Bulk facilities: From the matrix on the following page, select the "Site Considerations" line which most closely correlates with the application being considered and apply the "Physical Security Safeguards" indicated.

SITE CONSIDERATIONS			PHYSICAL SECURITY SAFEGUARDS
Territorial Status	**Clearance Status**	**Operational Status**	
U/F	A	C	1
U/F	M	C	1, 2
U/F	N	C	1, (4 or 5), 6, 7
U	A	L	1, 3, (4 or 5), 6
U	M	L	1, 2, 3, (4 or 5), 6, 7
U/F	N	L	1, 3, (4 or 5), 6, 7
F	A	L	1, 3, (4 or 5), 6
F	M	L	1, 2, 3, (4 or 5), 6, 7
U/F	-	V	1, 3, (4 or 5), 6, 7

LEGEND:

"Site Considerations" Symbols

Territorial Status

U - U.S. territory and sites on foreign soil where the responsible U.S. commander has the legal right to control access.

F - U.S.-occupied sites on foreign soil where the responsible U.S. commander does not have the legal right to control access.

Clearance Status

A - All persons having unrestricted access to the space are appropriately cleared; persons who are not appropriately cleared must be escorted.

M - At least one appropriately cleared person is continuously present in the space when the space is manned.

N - No appropriately cleared individuals are present when the space is manned.

ANNEX P

"SPECIAL" PHYSICAL SECURITY SAFEGUARDS FOR DoD BLACK BULK FACILITIES

Operational Status

C - The site is continuously manned.

L - The site is manned for some part of each working day, but is not continuously manned.

V - The site is normally unmanned.

"Physical Security Safeguards" Symbols

1 - Measures shall be taken to ensure that only authorized individuals are allowed unrestricted access to the space (e.g., doors and windows locked, visitors identified and escorted, and access lists maintained) .

2 - An appropriately cleared person shall be responsible for ensuring that uncleared personnel who are allowed access to the space are not afforded the opportunity to remove the crypto-equipment, to conduct a detailed external or any internal examination of it, or to extract key from it.

3 - The space shall be constructed to provide physical barriers to unauthorized access to the crypto-equipment.

4 - An approved mechanism shall be used to inhibit unauthorized removal or modification of an installed crypto-equipment or the extraction of its key.

5 - Operational crypto-equipment shall be installed in security containers approved by DIRNSA for storage of operational crypto-equipment. All extraneous holes and spaces around cable entrance points shall be sealed with an approved epoxy material. These containers shall not be used for storage of future keying material or COMSEC maintenance manuals.

6 - Open storage of keying material and COMSEC maintenance manuals is **prohibited**.

7 - Crypto-equipment employed must meet approved NSA standards for resistance to key extraction.

ANNEX Q

GENERATING STATION OTAR AND OTAT LOG

The form on the reverse side of this page is for your use to record montly OTAR/OTAT transactions. **Local reproduction of this form is authorized.**

Block Completion is identified, as follows :

1. **KEY SOURCE**
2. **SHORT TITLE**
3. **CLASS** (Classification of material sent/received)
4. **CA** (Controlling Authority of material sent/received)
5. **EFF PD** (Effective Period of material)
6. **STORAGE POSITION AND FILL DEVICE SERIAL** Number **(No.)**
7. **CIRCUIT** Identification **(I.D.) TRANSMITTED OVER RECEIVED** (Identify circuit used to transmit or receive)
8. **DATE/TIME OF TRANSMISSION**
9. **RECEIVING STATION(S)**
10. **ZEROIZED DATE/TIME**
11. **INITIALS** (Initials of the **two** personnel that **zeroized** the transaction)

CMS1 AMD3

CONFIDENTIAL (When Filled In)

GENERATING STATION OTAR / OTAT LOG FOR THE MONTH OF _____

1. KEY SOURCE	2. SHORT TITLE	3. CLASS	4. CA	5. EFF PD	6. STORAGE POSITION AND FILL DEVICE SERIAL NO.	7. CIRCUIT I.D. TRANSMITTED OVER RECEIVED	8. DATE/TIME OF TRANSMISSION	9. RECEIVING STATION(S)	10. ZEROIZED DATE/TIME	11. INITIALS
[redacted]										
[redacted]										

ANNEX R

RELAYING/RECEIVING STATION OVER-THE-AIR-TRANSFER (OTAT) LOG (R

The form on the reverse side of this page is for your use to record monthly OTAT transactions. **Local reproduction of this form is authorized.**

Block Completion is identified, as follows :

1. **KEY** Identification **(I.D.) SHORT TITLE**
2. **CA** (Controlling Authority of material sent/received)
3. **CLASS** (Classification of material sent/received)
4. **CIRCUIT KEY INTENDED FOR** (Identify System/Purpose)
5. **EFF PD** (Effective Period of material)
6. **DATE/TIME RECEIPT(R) TRANSMISSION(T)** (Identify date/time and annotate "R" for material received; "T" for material transmitted)
7. **CIRCUIT** Identification **(I.D.) TRANSMITTED OVER RECEIVED** (Identify circuit used to transmit or receive)
8. **STORAGE POSITION AND FILL DEVICE SERIAL** Number **(No.)**
9. **ZEROIZED DATE/TIME**
10. **INITIALS** (Initials of the **two** personnel that **zeroized** the key)

CONFIDENTIAL (When Filled In)

RELAYING/RECEIVING STATION OTAT LOG FOR THE MONTH OF _____

1. KEY I.D. SHORT TITLE	2. CA	3. CLASS	4. CIRCUIT KEY INTENDED FOR	5. EFF PD	6. DATE/TIME RECEIPT (R) TRANSMISSION (T)	7. CIRCUIT I.D. TRANSMITTED OVER RECEIVED	8. STORAGE POSITION AND FILL DEVICE SERIAL NO.	9. ZEROIZED DATE TIME	10. INITIALS	

PAGE _____ OF _____

CONFIDENTIAL (When Filled In)

ANNEX S

(R

CMS POINT OF CONTACT (POC) LISTING

* *

DIRECTOR, COMSEC MATERIAL SYSTEM (DCMS)

FACSIMILE: Secure: DSN: 764-2770 COMM: (202) 764-2770
Non-Secure: DSN: 764-0215 COMM: (202) 764-0215

MESSAGE ADDRESS: DCMS WASHINGTON DC//*See NOTE below*//

NOTE: Office codes for message traffic:

00 - CO
01 - XO
TD - Technical Director
10 - Administrative
20 - Policy, Procedures & Incidents
30 - Operations/Accounting
50 - Automated Information Systems
80 - Education, Training & Inspections

ETR MESSAGES: DCMS WASHINGTON DC//30/50//

MAILING ADDRESS: DCMS
ATTN (--)
3801 Nebraska Avenue NW
Washington DC 20393-5453

PRIMARY PHONE NUMBER(S):

DSN: 764-XXXX; COMM: (202) 764-XXXX

CO/XO -0399

10 -0499 (Administrative, Personnel)

20 -0352 (Plans, Policy & Incidents/PDSs)

30 -0606 (STU III Accounts)
-0525 (Vault)
-0317 (USMC, USCG, SPEWAR, CMIO, CRF, non-NAVY Accounts)
-0250 (Equipment; Submarine, Surface & Shore NAVY Accounts)
-0315 (Status & Stock Analysis)

ANNEX S

CMS POINT OF CONTACT (POC) LISTING

DCMS (continued)

50 -0704/0856/0877 (CARS, ANCRS)
-2819/2824 (NKDS)
-0340 (FEP Access)

80 -2837 (CMS Inspections, Training Visits, Education)

ACTION LINE -0245/46 (These numbers should be called during normal working hours (0630 - 1630 EST) **only** when unsure of what department you require assistance from. After hours, on holidays or weekends, an answering machine is set up on each line for action the next working day. The following information must be provided for action line response: Name of Command; CMS or SCA Account Number; Telephone Number (specify DSN or Commercial); Name of Person to Contact; and Subject or Reason for Inquiry.

NOTE: CARS FEP **toll free** access from within CONUS: 1-888-232-2700

COMMAND DUTY OFFICER - In the event you need immediate assistance (i.e., the issue **can not** wait to be resolved during normal working hours), contact NCTS Washington (**NOTE**

ANNEX S

CMS POINT OF CONTACT (POC) LISTING

DCMS (continued)

OPERATIONS DEPARTMENT (30):

-- Keying Material (KEYMAT) distribution or status (i.e., CMSR); COMSEC stock analysis; changes in the Highest Classification Indicator (HCI); LESS items; decommissioning; account establishment and disestablishment.

-- CMS material accounting (e.g., transaction number assignment/errors; ETRs; inventory report/reconciliation).

-- COMSEC equipment increases/decreases; related devices; maintenance manuals; operating instructions; equipment modifications; end-item accounting; and other equipment-related issues.

AUTOMATED INFORMATION SYSTEMS DEPARTMENT (50). COMSEC Automated Reporting System (CARS); Automated Navy COMSEC Reporting System (ANCRS); Front End Processor (FEP).

EDUCATION AND TRAINING DEPARTMENT (80). CMS Training Visits; CMS Inspections; suggestions or recommendations for improving the CMS Advice & Assistance (A&A) program, CMS inspections, or CMS training (including the CMS Custodian COI A-4C-0014 and Local Holder (LH) COI A-4C-0031). **NOTE**: CMS training visits are required every 18 months.

****

COMSEC MATERIAL ISSUING OFFICE (CMIO)

DSN: 564-7051/52/53 COMM: (804) 444-7051/52/53

FACSIMILE: Secure: Same as above

Non-Secure: DSN: 564-1745 COMM: (804) 445-1745

MESSAGE ADDRESS: CMIO NORFOLK VA//--//

00 - OIC
01 - Deputy OIC
10 - Administrative
11 - Command Chief
20 - Distribution
30 - Vault Officer
31 - Vault Supervisor

ANNEX S

CMS POINT OF CONTACT (POC) LISTING

CMIO (continued)

MAILING ADDRESS: OIC
CMIO Norfolk
8876 2nd Street
Norfolk VA 23511-3797

*** ***

CMS ADVICE AND ASSISTANCE (A&A) TRAINING TEAMS

ATLANTIC AREA

CMS AA WASHINGTON DC

DSN: 764-2837 COMM: (202) 764-2837

CMS AA NEWPORT RI

DSN: 948-3843/44 COMM: (401) 841-3843/44

CMS AA NORFOLK VA

DSN: 262-2084 COMM: (804) 322-2084

CMS AA MAYPORT FL

DSN: 960-6106 COMM: (904) 270-6106

EUROPEAN AREA

CMS AA ROTA SP

DSN: 727-3248 COMM: 011-34-56-823248

ANNEX S

CMS POINT OF CONTACT (POC) LISTING

A&A Teams (continued)

CMS AA NAPLES IT

DSN: 625-4234 COMM: 011-39-81-724-4234

PACIFIC AREA

CMS AA FAR EAST FE

DSN: 234-6037 COMM: 81-468-26-1911, Ext. 6037

CMS AA PEARL HARBOR HI

DSN: 471-2361 COMM: (808) 471-2361/62

CMS AA PUGET SOUND WA

DSN: 744-6950 COMM: (360) 396-6950

CMS AA SAN DIEGO CA

DSN: 522-1041/3078 COMM: (619) 532-1041/3078

NSA AND MILITARY CENTRAL OFFICE OF RECORD (CORs)

NSA COR

MESSAGE ADDRESS: DIRNSA FT GEORGE G MEADE MD//7131//

MAILING ADDRESS: ATTN Y131
National Security Agency
9800 Savage Road
Ft. Meade MD 20755-6000

ANNEX S

CMS POINT OF CONTACT (POC) LISTING

ARMY COR

MESSAGE ADDRESS: DIRUSACCSLA FT HUACHUCA AZ//SELCL-KPD-OR//

MAILING ADDRESS: Director, U.S. Army Communications Electronics Command
Communications Security Logistics Activity
ATTN SELCL-KPD-OR
Ft. Huachuca AZ 85613-7090

AIR FORCE COR

MESSAGE ADDRESS: DIR CRYPTO MGT KELLY AFB TX//LTMKC//

MAILING ADDRESS: SA-ALC
ATTN LTMKC
230 Hall Blvd Suite 107-108
San Antonio TX 78243-7056

****

MISCELLANEOUS POINT OF CONTACT (POC)

COMMONLY MISUSED DIRNSA INSECURITY PLA:

DIRNSA FT GEORGE G MEADE MD//V51A//

****

ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS)

STU-III REKEY: DSN: 936-1810 COMM: (410) 526-3200

Toll-FREE within CONUS: 1-800-635-6301

USER ASSISTANCE: DSN: 238-4000 COMM: (410) 526-3207

Toll-FREE within CONUS: 1-800-635-5689

ANNEX S

CMS POINT OF CONTACT (POC) LISTING

EKMS (continued)

MAILING ADDRESS: EKMS
P O Box 718
Finksburg MD 21048-0718

FACSIMILE: Secure:
DSN: 238-4108/27
COMM: (410) 526-3108/37

Non-Secure:
DSN: 238-4172
COMM: (410) 526-3172

****

NAVAL COMMAND, CONTROL AND OCEAN SURVEILLANCE CENTER RESEARCH DEVELOPMENT TEST AND EVALUATION DIVISION (NRAD)

NRaD, Code 87, is the Software Support Activity (SSA) for all subsystems of the Navy Key Management System (NKMS) to include: NKDS, WETS, CARS, ANCRS. Account holders should direct all LMD system technical questions (i.e., application programs, communications, interfacing issues) or questions regarding LMD installation, repair or upgrades, as well as, LMD suite disposition instructions if decommissioning, to:

NKMS Technical Help Desk at 1-800-656-7201

DCMS and CMIO (**only)** personnel requiring assistance or to report system-level problems are requested to contact the NKMS SSA Help Desk at (619) 553-9584.

****

NISE EAST CHARLESTON SC

NISE EAST Charleston combines the services of the present Information Security (INFOSEC) help line with those of the Naval Key Management System (NKMS) help line. This help line receives calls 24 hours a day and is manned a minimum of twelve hours per day, Monday through Friday.

HELP DESK PHONE: DSN: 563-8878/8879
COMM: (803) 974-5426
TOLL FREE: 1-800-304-4636

ANNEX S

CMS POINT OF CONTACT (POC) LISTING

MISC (continued)

NON-SECURE FAX: DSN: 563-2030, Ext. 5461
COMM: (803) 974-4495

E-MAIL: INFOSEC.NOSC.MIL.

NAVAL ELECTRONIC BULLETIN BOARD: DSN: 563-8880
COMM: (803) 974-4495
TOLL FREE: 1-800-494-9947

MESSAGE ADDRESS: NISEEAST CHARLESTON SC//40C//

MAILING ADDRESS: Commanding Officer
Code 42
NISE EAST
4600 Marriott Drive
North Charleston SC 29406

ANNEX T

RETENTION PERIODS FOR CMS FILES, RECORDS, AND LOGS (R

1. **Purpose**. To prescribe the minimum retention periods for CMS files, records, logs (both active and inactive) used in managing a CMS account.

2. **Retention Periods**. The retention periods indicated in this annex are **minimum** requirements. The destruction of inactive files, records, and logs should be accomplished as soon as practical after the minimum retention period.

a. **CMS 17 LOCAL CUSTODY CARDS**. Retain for 90 days after supersession.

b. **SF 153 LOCAL CUSTODY DOCUMENTS**. Retain for 90 days after supersession.

c. **LETTERS OF APPOINTMENT**. Retain for two years from the date an individual has been relieved of his/her duties.

d. **RUNNING INVENTORY (R/I)**. Retain pages removed and replaced because all listed items have been disposed of for 90 days.

NOTE: ANCRS Users: See subparagraph n.

e. **INVENTORY REPORT**:

(1) Retain file copy of Fixed-Cycle/Combined in the Chronological File for two years (includes inventories by Local Holder/User).

(2) Retain working copy of Fixed-Cycle/Combined until subsequent SF 153 reflects "original" submission as "reconciled."

(3) Retain Special (e.g., Change of Command and/or Custodian) until subsequent Fixed-Cycle/Combined inventory is reconciled by DCMS.

f. **WATCH-TO-WATCH INVENTORY SHEETS**. Retain for 30 days beyond last recorded inventory date on the sheet.

g. **TRANSACTION LOG**. Retain for two years. (**NOTE**: Pages being replaced may be destroyed when accuracy of new page(s) has been verified.)

NOTE: ANCRS Users: See subparagraph n.

ANNEX T

RETENTION PERIODS FOR CMS FILES, RECORDS, AND LOGS (R

h. **TRANSFER, POSSESSION, CONVERSION, and RELIEF FROM ACCOUNTABILITY** (i.e., SF 153 REPORTS). Retain for two years.

i. **DESTRUCTION RECORDS** (e.g., SF 153, CMS 25 (or equivalent form used to record segmented destruction) SF 153). The following pertains:

(1) Retain for two years only for SECRET and above.

(2) Retention and documentation of CONFIDENTIAL and below material is at the discretion of the CO/OIC since there is no prescribed requirement to document destruction of CONFIDENTIAL and below material.

NOTE: Copies of required destruction reports used by Local Holders/Users when the original is forwarded to the CMS Account Custodian will be retained or disposed of in accordance with local command directives.

j. **CORRESPONDENCE and MESSAGES**:

(1) Retain GENERAL messages relating only to account holdings and all GENERAL messages for policy/procedures until authorized for destruction by the originator.

(2) Retain general correspondence and all other messages relating to only account holdings for two years.

k. **DIRECTIVES and INSTRUCTIONS**. Retain required items related to your account until cancelled or superseded.

l. **RECEIPTS** (e.g., DCS, mail). Retain for 1 year.

m. **RUNNING INVENTORY (R/I) and TRANSACTION LOG** (for **ANCRS Users**). ANCRS Users will maintain copies of their R/I and transaction log IAW the following:

TYPE COMMAND	FREQUENCY OF PRINTOUTS	RETENTION PERIOD
Submarine	Prior to putting to sea.	Destroy when replaced with updated versions.
Surface or Deployed Mobile Units	Once a month.	Destroy when replaced updated versions.

ANNEX T

RETENTION PERIODS FOR CMS FILES, RECORDS, AND LOGS (R

TYPE COMMAND	PRINTOUTS	FREQUENCY OF RETENTION PERIOD
Shore or Non-Deployed Mobile Units	Once every 3 months.	Destroy when replaced with updated versions.

n. **CMS UPDATES**. Retain for two years. (A

ANNEX U
CMS TRANSACTION LOG

1. ACCOUNT NUMBER _____ **2. YEAR** _____

3. TRANS NO.	4. COMMAND TITLE	5. ACCOUNT NO.	6. DATE MM/DD

ANNEX U
CMS TRANSACTION LOG

1. **Purpose:** The CMS Transaction Log is used to record and assign sequential, transaction number (TN) to accounting reports which are forwarded to the DCMS COR.

2. **CMS Transaction Numbers (TNs):** CMS TNs maintain the continuity of COR transactions within each CMS account, and provide a means of verifying individual account records.

3. **Assigning Transaction Numbers:**

a. Manually-assigned TNs: The following procedures are applicable for manually assigning TNs to COR accounting reports.

(1) The first digit of the TN will always be the last digit of the calendar year (CY) in which the accounting report is generated (e.g., 2xxxxx or 3xxxxx for CY 1992 and 1993, respectively).

(2) The remaining fi ve digits must run in consecutive numerical sequence beginning with 00001. Consequently, the first TN assigned to the first COR accounting report originated by all CMS accounts in 1993 would be 300001. The tenth TN of CY 93 would be 300010.

b. ANCRS-assigned TNs: When using ANCRS, a TN will be automatically generated, assigned to the accounting report, and recorded in the Transaction Log. ANCRS -generated TNs are displayed in the Transaction Log as follows:

(1) The Julian Date will be expressed in four digits; the first digit will be the last digit of the CY and the next three digits the actual Julian Date (e.g., 31 May 1993 would be listed as: "3151").

(2) ANCRS-generated TNs consist of only the last five digits of a six-digit TN sequence. However, in the Transaction Log, TNs will be truncated to four digits when assigning TNs from 1-99, and five digits when assigning TNs from 100-999. This is done in order to conserve computer disk space. For example, TN 34 generated on 30 May 1993, would be displayed in the

ANNEX U

CMS TRANSACTION LOG

Transaction Log as the last digit of the CY, followed by the Julian Date, a hyphen, leading zeros, TN 34, and would appear as follows: "3151 -0034." TN 121, generated on 15 August 1993, would be displayed as: "3228 -00121."

4. **Preparing the Manual CMS Transaction Log:** The following procedures are applicable for recording and assigning TNs to manually prepared COR accounting reports and the Transaction Log:

a. **Account Number (Block 1):** Enter the six -digit account number of the CMS account preparing the accounting report.

b. **Year (Block 2):** Enter CY (e.g., 1993).

c. **Transaction Number (Block 3):** Enter the six -digit TN.

d. **Command Title and Account Number (Blocks 4 and 5):**

(1) For SF 153 Possession and Conversion Reports, the Block 4 and 5 entries will be the command title and CMS account number of the originating command.

(2) For SF 153 Transfer, Destruction, Relief from Accountability Reports, the Block 4 and 5 entries will be the command title and CMS account number of the other unit involved in the transaction.

NOTE: 1. Do not forward destruction reports to DCMS unless specifically directed to do so by DCMS.

2. CMS account inventories are not transactions and will not be logged in the Transaction Log or assigned a TN.

e. **Date (Block 6):** Enter the month and day of the report (i.e., MM/DD). If the SF 153 is a DCMS reportable destruction report, the date must either be the date the material listed was actually destroyed or, if used to summarize local destruction records, the date the consolidated destruction report was prepared.

ANNEX U

CMS TRANSACTION LOG

5. **TN Errors:** If the CMS Custodian discovers an error was made in assigning a TN to a COR accounting report, (e.g., a TN was duplicated or skipped, digits transposed) or if a TN submitted for processing must be cancelled, the Custodian must notify DCMS//30// using one of the following:

a. CARS,
b. Facsimile,
c. Message,
d. Letter.

(1) The Custodian must advise whether the TN should be reassigned, cancelled, or otherwise changed.

(2) If DCMS discovers the error, DCMS will notify the command.

6. **Retention of the Transaction Log:** At the end of each CY, the Transaction Log must be annotated to certify that the last TN listed is the last TN used by the account during that CY. The log will be retained in the chronological file in accordance with Annex T.

ANNEX V

COMPLETING LOCALLY-PREPARED SF 153 COMSEC MATERIAL ACCOUNTING REPORTS

1. **Purpose:** To provide general guidance for completing SF 153 COMSEC material accounting reports.

2. **Preprinted SF 153 COMSEC Material Reports:**

a. There are currently two versions of the preprinted SF 153 COMSEC Material Report authorized for use; one reflects a revision date of 9-79 and the other 9-88.

b. Both versions contain identical data blocks of information but are assigned different numbers. The example SF 153 and amplifying data contained in this Annex addresses revision 9-88.

c. ANCRS-generated SF 153s conform to revision 9-88.

3. **Verifying For Completeness and Accuracy:**

a. The accuracy of accounting reports is an extremely important aspect of account management. Consequently, prior to forwarding a report, the completeness and accuracy of all information must be verified.

b. Incomplete/erroneous COR accounting reports (e.g., missing addresses, dates, transactions numbers, signatures or the report contains errors in the short title(s) or accounting data) forwarded to DCMS cannot be processed until all errors or omissions are corrected.

c. Changes or corrections to a SF 153 COMSEC Material Accounting Report must be reported to DCMS//30// via message or facsimile.

4. **Assigning Transaction Numbers (TNs):**

a. CMS TNs maintain the continuity of COR reportable transactions within each CMS account and provide a means of verifying individual account records.

b. With the exception of the DCMS-Generated SF 153 Inventory Report, all other DCMS reportable accounting reports must be assigned a TN in accordance with Annex U.

ANNEX V

COMPLETING LOCALLY-PREPARED SF 153 COMSEC MATERIAL ACCOUNTING REPORTS

c. TN errors must be corrected in accordance Annex U of this manual.

5. **Line Entries on SF 153 Accounting Reports:**

a. Material must be listed one item per line on all SF 153 Accounting Reports.

b. If multiple copies of an edition of an AL 1 short title are being reported and the accounting numbers are in consecutive order, one line entry should be used (e.g., USKAA 888 AB 344, 345, and 346 may be listed as: "USKAA AB 888 344-346.") (R

c. If accounting numbers are not in consecutive sequence (i.e., sequential number series is broken), a separate line entry is required for each.

d. For AL 2 and AL 4 material (accountable by quantity), list multiple copies of the same short title and edition as a single consolidated line entry.

e. Different editions of the same short title must be listed separately.

f. **Close-out Line Entries on Accounting Reports:**

(1) Immediately below the last short title entry on the last (or only) page of an SF 153 Accounting Report, enter "TOTAL LINES: ___ TOTAL QUANTITY: ___" as a single line entry.

(2) The total lines entry is the total of all short title line entries.

(3) The total quantity entry is the total of the quantity column for all short titles listed on the report.

6. Signature Requirements:

a. Inventory, Destruction, and Relief from Accountability Reports:

(1) Require the signature of two Custodians or a Custodian and a properly cleared witness, and the Commanding Officer/OIC/SCMSRO, as appropriate:

(2) In the absence of the Commanding Officer, the Executive Officer is authorized to sign accounting reports as "Acting" Commanding Officer.

ANNEX V

COMPLETING LOCALLY-PREPARED SF 153 COMSEC MATERIAL ACCOUNTING REPORTS

(3) Accounting reports which are signed by the SCMSRO must be annotated to reflect "Staff CMS Responsibility Officer" vice by direction or acting.

b. Reports listing SAS/TPC Material:

(1) SF 153 Transfer and Destruction reports which list SAS/TPC material must be signed by two members of the SAS/TPC team.

(2) SAS/TPC accounting reports must be given to the CMS Custodian for use in reporting the transfer or receipt of SAS/TPC material to DCMS. (**NOTE:** CJCSI 3260.1 contains basic accounting and control guidance for SAS/TPC material.) (R

c. Other Reports:

All other accounting reports require only the signature of the CMS Custodian and/or an Alternate and a properly cleared witness.

d. All accounting reports submitted to DCMS must be signed and be original copies.

e. Signatures generated by means of a signature stamp or other signature device are not permitted.

f. A carbon copy or a reproduced copy of an original accounting report is acceptable for the following two purposes:

(1) Local record retention; and,
(2) Receipt to the originator of a material transfer.

NOTE: Signatures on reproduced accounting reports must be clearly visible.

g. Signature Data: In addition to the written signature, the name, rank/rate/grade, and service of each person who signs an accounting report must be typed, printed, or stamped in the appropriate block(s) of the report.

ANNEX V

COMPLETING LOCALLY-PREPARED SF 153 COMSEC MATERIAL ACCOUNTING REPORTS

7. **Completing Multi-Page SF 153 Reports**:

a. When a multi-page SF 153 is used, the close-out line information ("TOTAL LINES: TOTAL QUANTITY:") must be entered only on the last page (immediately below the last short title entry).

b. Blocks 2-6 on each page of a multi-page accounting report must be completed.

c. Only one TN may be assigned to a multi-page accounting report. Consequently, all material listed in the report is treated as a single transaction.

d. Annotate the consecutive page number in block 17 on each page of the report and record the total pages comprising the multi-page report on the last page (e.g., 10 of 10).

e. Signatures are required only on the last page of a multi-page report.

8. **Completing Data Blocks 1-17 of the SF 153:**

a. **Block 1 - Type of Report:** Indicate the type of report by placing an "x" in the appropriate box. If the specific type of report being prepared is not listed, place an "x" in the box marked "Other." Next to this box, annotate/type the type of report (e.g., Possession).

b. **Block 2 - From:** Enter your account command title, complete mailing address, and CMS account number.

NOTE: If a "Local" SF 153 Accounting Report (e.g., local destruction, local inventory) is being prepared, the CMS account number may be omitted.

c. **Block 3 - Date of Report:** Enter the date as year, month, and day (e.g., 930815). Reports generated by ANCRS will display the last digit of the calendar year and the Julian date following the year, month, day entry. Complete Block 3 as indicated below for the following reports:

(1) Transfer reports: Completed by the originator of the transfer and must reflect the date that the report was actually prepared.

ANNEX V

COMPLETING LOCALLY-PREPARED SF 153 COMSEC MATERIAL ACCOUNTING REPORTS

(2) Receipt reports: Completed by the recipient of an SF 153 Transfer Report and must reflect the date the SF 153 is being signed.

(3) Destruction reports: Completed by the originator and must reflect the date on which the material listed was actually destroyed. If report is being used to consolidate other destruction records (e.g., from LHs or Users), date of report preparation is acceptable.

(4) Possession, Relief from Accountability, Conversion, and Inventory Reports: Completed by the originator and must reflect the date the SF 153 is being signed.

d. **Block 4 - Outgoing TN:** Originator will assign a COR Reportable TN from the CMS Transaction Log ONLY if the SF 153 is to be forwarded to DCMS. Otherwise, this block may be left blank or assigned a local TN.

e. **Block 5 - Date of Transaction:** For recipients of Transfer Reports, enter the date the SF 153 is signed. Leave this block blank for Destruction, Transfer, Possession, Conversion, Inventory, and Relief from Accountability Reports.

f. **Block 6 - Incoming TN:** Recipient will assign a COR Reportable TN from the CMS Transaction Log ONLY if the SF 153 is to be forwarded to DCMS. Otherwise, this block may be left blank or assigned a local TN.

g. **Block 7 - To:**

(1) For SF 153 Transfers: Enter the command identification, complete mailing address, and the CMS account number of the unit to which the material is being sent. (**NOTE:** When the intended recipient is a ship, include the type and hull number of the ship instead of geographic location.)

(2) For SF 153s Used to Issue Material on Local Custody: Enter the command title or identification of LH/User.

(3) For SF 153 Possessions, Conversion ADD, and Inventories (Special) Reports: Enter the same data as entered in Block 2. (NOTE: Blocks 2 and 7 must reflect the same information.)

ANNEX V

COMPLETING LOCALLY-PREPARED SF 153 COMSEC MATERIAL ACCOUNTING REPORTS

(4) For SF 153 Conversion DELETE and Relief from Accountability Reports: Enter: "CMS REMOVAL" and account number: 095999.

(5) For SF 153 Destructions: If preparing the report for submission to DCMS, insert "CMS DESTRUCTION" and insert the account number 095997. Otherwise, leave blank.

h. **Block 8 - Accounting Legend Codes:** Leave blank.

i. **Block 9 - Short Title/Designator-Edition:** Enter the short title(s) and accounting data for the applicable COMSEC material in accordance with Article 225.

(1) Block 9 close out line: Immediately below the last short title line entry, enter: "TOTAL LINES____TOTAL QUANTITY____."

(2) Block 9 special remarks: Below the "TOTAL LINES/TOTAL QUANTITY" entry, the following remarks, though not all inclusive, should be entered as applicable:

(a) Destruction Reports: Annotate the destruction authorization (e.g., CSMR, originator and date-time-group of message).

(b) Transfer Reports: Cite transfer authorization in accordance with Article 733. Additionally, if the transfer is an Inter-Service transfer, ensure entry of transfer statement in Article 733 a.

(c) For ANCRS-generated SF 153s, special remarks are automatically entered based on the type of report generated. If the remarks are not applicable, manually modify or correct as appropriate.

j. **Block 10 - Quantity:** Enter the quantity of items reflected in Block 9.

k. **Block 11 - Accounting numbers (beginning/ending):** Enter the accounting number(s) of the short title(s) listed in Block 9. If the quantity is one, the beginning column may be left blank and the accounting number entered in the ending column.

ANNEX V

COMPLETING LOCALLY-PREPARED SF 153 COMSEC MATERIAL ACCOUNTING REPORTS

l. **Block 12 - ALC:** Enter the AL Code of the short title.

m. **Block 13 - Remarks:** Enter any information considered pertinent to the report.

n. **Block 14 - Type of action taken:** Place an "x" in the appropriate box. If the type of action taken is not indicated, leave all boxes blank.

o. **Block 15 - Authorized recipient:** For all reports, less transfers, enter "CMS Custodian."

(1) Blocks 15a & 15b: Signature of Custodian and rank/grade for all reports, less transfers. (**NOTE**

1. **General**:

a. This Annex prescribes the policy and procedures for formatting and electronically forwarding selected Central Office of Record (COR) accounting reports via an Electrical Transaction Report (ETR).

b. The **primary** transmission path for submitting ETRs is via the COMSEC Automated Reporting System (CARS). As an alternative, ETRs may also be prepared in message format and submitted via the General Service (GENSER) AUTODIN Communications Network.

c. The Automated Navy COMSEC Reporting System (ANCRS) will automatically format ETR data fields for accounts that use the ANCRS software package. Commands not using ANCRS must manually prepare ETRs using the procedures in this Annex.

d. The procedures described herein for formatting data fields are used for all ETRs regardless of the transmission path. Procedures and example ETRs will first be presented in message format and then an example of the same ETR will be shown as automatically formatted by ANCRS for transmission via CARS. Where applicable, procedural differences (due to the transmission path) will be noted.

e. Annex F contains procedures for accessing CARS and using the many features that this system provides for exchanging CMS-related information to and from the DCMS database using a personal computer (PC) and a Secure Telephone Unit (STU -III).

f. Procedures in this Annex will be presented in the following order:

(1) General policy/procedures for ETRs.

(2) Receipt ETR procedures (Tab 1).

(3) Transfer/Receipt ETR procedures (Tab 2).

2. **Policy**:

b. Generally, the only time the above COR reports will be mailed to DCMS is when an account cannot forward reports via CARS or, for messages, when MINIMIZE or Emission Control (EMCON) is in effect.

(1) When MINIMIZE or EMCON is in effect, ETR message procedures are suspended.

(2) The above reports, for accounts unable to use CARS, must then be mailed to DCMS and annotated with EMCON or MINIMIZE, as applicable, on the completed SF 153.

3. **Definition and Purpose**:

a. ETRs are specially formatted data fields transmitted directly into the DCMS COR database.

b. ETRs, when received and properly formatted, (R automatically update the holdings of a CMS account and eliminate manual data entry by DCMS. Automated processing significantly increases the accuracy of material held in an account by reducing the time lag between documentation preparation and receipt by DCMS (e.g., line outs on the DCMS-generated SF 153 Inventory Report will be reduced).

4. **Limitations**:

a. ETR procedures are not authorized for STU -II/III equipment or keying material.

b. ETR procedures are not authorized for material received from the following:

(1) Army and Air Force accounts.

(2) NSA 800000 through 870000 accounts.

(3) Contractor accounts (e.g., commercial vendors).

5. **General ETR Procedures and Formatting Requirements**:

a. Prior to transmitting an ETR to DCMS, the Custodian must verify, using a copy of the ETR, that the information in the ETR is accurate and has been correctly formatted.

b. If an error is discovered after transmitting an ETR, do not retransmit the ETR; forward an administrative message to "DCMS WASHINGTON DC//30//" citing the TN(s) and message DTG (for (R a message ETR) or the CARS destination file name contained in the original ETR (for CARS ETRs) and identify the error(s). DCMS will then take corrective action.

c. ETR data fields must be precisely formatted as detailed in this Annex. Successful computer processing of ETRs is directly dependent on absolute adherence --no deviation --to formatting requirements. The DCMS computer will only recognize and process automatically those ETRs which are correctly formatted. Any deviation from formatting requirements will result in the ETR being "dumped" to the error queue for manual processing.

d. All entries which require a date must be entered in year/month/day (YYMMDD) or year/month (YYMM) format with no spaces or slashes (e.g., 930624 or 9306).

e. A slash (/) is used to separate one field or element from another and the question mark (?) is used to indicate that an element of a short title/data field is not present/used.

NOTE: Custodians are **strongly** encouraged to provide a copy of ETR procedures and message examples to their servicing communications center. The majority of errors encountered to date have been attributed to communications center personnel arbitrarily making "corrections" to ETRs that were properly drafted/formatted by the Custodian.

6. **General Formatting Procedures for Short Titles**:

title as required. For example, if the "system" field of a short title you are reporting contains only three characters, you would enter only three characters.

d. Do not insert extra characters/digits in order to use the entire space allocated for a field except for DIRNSA TNs.

e. Do not insert line spaces between format lines or indent format line entries or place them in paragraph form. Enter the required information in the ETR data fields exactly as shown in the ETR examples.

NOTE: Commands who use the ANCRS program and forward their ETRs via CARS may disregard formatting requirements detailed in this Annex since ANCRS automatically and correctly formats ETR data fields for transmission via CARS.

7. **Format for Listing Short Titles**:

a. The format for short titles in ETRs is divided into six separate fields, each separated by a slash (/), and must be listed in the following sequence:

SYSTEM/CLASS/NUMBER/EDITION/AMENDMENT/FUTURE USE
(1) (2) (3) (4) (5) (6)

(1) **System**: The first field of a short title is the system and is limited to six (6) characters. The system is the first group of letters and/or digits found in a short title (e.g., AMSG, AKAI, KAM, KG, USKAK, USKAT).

(2) **Class**: The second field of a short title is the class and is limited to five (5) characters. The class is a group of letters and/or digits found between the system and the number of a short title, and will be entered immediately to the right of the slash (/) separating the system field from the class field. In the example, "USKAC D 166," the "D" is the class and would be entered as: "/D/."
(**NOTE**: The majority of short titles do not have a class element. Refer to your DCMS-generated SF 153 Inventory Report as (R
these reports list short titles and their various elements in the

For example, to report a transaction involving the short title, "USKAT 2044," the number "2044" would be entered as: "/2044/."

(4) **Edition**: The fourth field of a short title is the edition and is limited to six (6) characters. The first letter of the edition starts immediately to the right of the slash (/) separating the number field from the edition field. For example, in "KAM 15 B," "B" is the edition and would be entered as: "/B/."

(5) **Amendment**: The fifth field of a short title is the amendment field and is limited to 12 alphanumeric characters. The amendment field information will vary, as explained below, and will start immediately to the right of the slash (/) separating the edition field from the amendment field.

(a) The amendment field is used for amendments, reprints, corrections, equipment mode designators, equipment modifications, and other information that is part of a short title. In the example, "CSP 6675 A MASTER REEL," "MASTER REEL" does not fall in any of the above categories. However, the information is part of the short title and must be included as an entry in the amendment field.

(b) To enter an amendment in the amendment field, you must include the abbreviation "AMEND" followed immediately by a two-digit amendment number. All amendment numbers must be entered as two-digit numbers without any spaces. For example, "KAM 154A AMEND 4," the "AMEND 4" would be entered as: "/AMEND04/."

(c) To enter an equipment mode designator in the amendment field, use the first four positions of the amendment field. Insert a dash (-) in the first position, a zero (0) in the second position, and then enter the mode designator in the third and fourth positions. For example, "KG -36 B-54," the "54" is the equipment mode designator and would be entered as: "/-054/."

(6) **Future use**: The sixth field of a short title is programmed for future use. However, it is a required field to permit computer processing of ETRs. Always enter a question

c. If you are in doubt as to how a short title should be listed, refer to the short titles and the identification of the short title fields in the heading of the DCMS-generated SF 153 Inventory Report or call DCMS//30//. The DCMS-generated SF 153 Inventory Report presents short titles and their various elements in the proper sequence.

(D

8. **Message Format for ETRs:**

a. The DCMS COR computer has been programmed to recognize and process GENSER messages formatted with and without GENADMIN formatting procedures. ETR messages can be submitted in either format. Example 1 in Tab 1 is an example of a Receipt ETR message in non -GENADMIN format.

b. ETR message format must be in strict compliance with JANAP 128/ACP 121, unless the command is authorized to forward messages using the NTP -4/modified ACP 126 procedures to a NAVCOMPARS for conversion to JANAP 128 format and subsequent delivery via the AUTODIN Communications Network. Example 3 in Tab 1 and Example 1 in Tab 2 are examples of a Receipt ETR and a Transfer/Receipt ETR message in JANAP 128 and ACP 126 formats, respectively.

9. **Message Heading Format for ETRs**: The message heading for ETR messages must be formatted as follows:

a. **Precedence**: R (routine)

b. **Language Media Format** (LMF): TT (R

(D

c. **Message Content Indicator Code (CIC)**: ZYUW (R

d. **Originating Message Address:** Use your standard Plain Language Address (PLA)

e. **Action Addressee:** DCMS WASHINGTON DC. (**NOTE**:

g. **Classification**:

(1) ETRs will normally be unclassified except those which list SAS/TPC short titles or contain classified remarks.

(2) ETR messages which report SAS/TPC short titles will be classified in accordance with CJCSI 3260.1. (R

NOTE: Classified ETRs must be sent via a classified message or via the CARS SECRET PC or FEP.

h. **Standard Subject Identification Code** (SSIC): N02283.

i. **Subject**: COMSEC MATERIAL ETR.

j. **Text**: The text of each ETR message must be specifically formatted according to the type of accounting report involved. The specific format for each type of ETR is provided in the Tabs of this Annex.

D)

10. **Documentation and Reporting Procedures:** Custodians must read and be familiar with the applicable documentation and reporting requirements for ETR-eligible accounting reports that are detailed in this publication prior to preparing an ETR.

11. **Accuracy**: It is absolutely imperative that ETRs be formatted accurately; this fact cannot be overemphasized. DCMS, as the DON COR for over 1000 CMS accounts and 900 STU-III accounts, processes hundreds of thousands of accounting (R reports annually. The expanding use of automated processing procedures/systems mandates attention to detail and strict observance of procedural requirements. **Successful processing of ETRs is directly dependent on formatting accuracy**.

NOTE: At the end of each line of an ANCRS generated ETR, the account number and the last four digits of the TN will appear commencing in column 71 (e.g., 078002/5697). This repetition of the account number and TN is a "check and balance" function within the ANCRS program. The repeating

1. **Purpose**: The Receipt ETR is used to report to DCMS (and the originator of the shipment) the receipt of AL 1, 2, or 4 COMSEC material from the following accounts only:

a. 078000 (DCMS)
b. 078002 (CMIO Norfolk)
D)
d. 360109 (NAVCOMTELSTA Sicil y)
e. 880093 (DIRNSA)
f. 880099 (DIRNSA)

2. **Policy**:

a. AL 1, 2, or 4 COMSEC material received from the above accounts must be receipted for via a Receipt ETR transmitted via CARS or message. (R

b. A Receipt ETR must be prepared and transmitted by the recipient of a shipment within 96 hours of receiving a shipment. (NOTE: See timeframe for reporting receipt in Article 742 b.)

3. **Receipt ETR Format**: The Receipt ETR consists of two format lines:

a. "R1" : Contains receipt data.

b. "R3" : This line identifies the names and SSNs of the two individuals receipting for SAS/TPC material. The "R3" line is used only when receipting for SAS/TPC material from DIRNSA.

4. **Reporting/Documentation Requirements**: The method used to transmit the Receipt ETR (i.e., CARS or message) will determine how documentation requirements (i.e., handling of the SF 153) are fulfilled. The following options are provided:

a. ETR Sent via CARS :

(1) Complete the SF 153 and return it to the originator

b. ETR Sent via Message :

(1) Include the originator of the shipment as an addressee, except for DIRNSA, on the Receipt ETR message.

(2) Compl ete the SF 153 and attach a copy of the Receipt ETR message and file them in the Chronological File.

NOTE: Do not forward copies of corresponding SF 153s to DCMS for Receipt ETRs submitted via CARS or message.

5. **Discrepancies**:

a. Discrepancies discovered upon receiving/opening a shipment such as missing/extra material, wrong serial number(s), pagecheck errors, damaged inner packages, packages showing evidence of tampering, and other discrepancies noted in the material itself or in the shipping containers/methods are not to be reported in an ETR.

b. Report discrepancies in accordance with the guidance contained in Article 742.c.

6. **Multiple Receipt ETRs**: Multiple receipts (i.e., receipts conducted under more than one transaction number) may be combined and reported in a single ETR. Each Receipt ETR must start on a separate line and begin with "ET/R1/." (**NOTE**: Example 3 shows multiple receipts in a single ETR message.)

7. **Receipt ETR Format**:

a. This Tab will show a Receipt ETR in message format and then show the same ETR as it would be formatted automatically by ANCRS for transmission via CARS.

b. After the example Receipt ETR formatted by ANCRS will be an explanation for the data fields in each of the format lines. The explanations pertain to data fields formatted by ANCRS and to those that are manually prepared.

d. Format line numbers and numbers enclosed in parentheses under the ETR data fields in the examples that follow are for explanation purposes only. They must not be used in ETRs that are transmitted via CARS or in message format.

8. **Receipt ETR Examples and Formatting Explanations:**

a. **EXAMPLE 1: Receipt ETR Message:**

```
RTTUZYUW RUHPDEA3280 2721844 -UUUU-SUU.                          (R
ZNR UUUUU
R 301845Z AUG 96 ZYB
FM USS LITTLE ROCK
TO DCMS WASHINGTON DC                                            (R
INFO CMIO NORFOLK VA//20//
BT
UNCLAS // N02283 //
SUBJ: COMSEC MATERIAL ETR
                    (FORMAT LINE 1)

ET/R1/078002/960822/601248/345278/960829/600086/26/89
(1)(2)  (3) (4)   (5)   (6)   (7)   (8) (9)(10)

                (FORMAT LINE 3)

ET/R3/XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
 (11) [------- -------(12)------- ----------]
```

NOTE: There is NO format line 2 (ET/R2/) in a Receipt ETR.

b. **EXAMPLE 2: Receipt ETR Formatted by ANCRS for Transmission via CARS:**

(FORMAT LINE 1)

ET/R1/078002/960822/601248/345278/960829/600086/26/89

c. **Explanation for Format Line 1 Text Entries**:

(1) ET/ -- "ET" is the computer flag that stands for electrical transaction.

(2) R1/ -- "R" indicates receipt and "1" represents the format line number.

NOTE: SF 153 block number references cited below are keyed to the latest SF 153 form (Rev. 9/88).

(3) CMS account number of the command that transferred the material. This field is limited to six digits. Corresponds to the account number in Block 2 of an SF 153.

(4) Date of report. This field is limited to six digits. Corresponds to the date entered in Block 3 of an SF 153 (e.g., 960527).

(5) Transaction number of the originating command. This field is limited to six digits. Corresponds to the number entered in Block 4 of an SF 153. (NOTE: If the material is from DIRNSA, the last digit of the CY must precede the 5 -digit DIRNSA TN.)

(6) CMS account number of the recipient. This field is limited to six digits. Enter your account number (Block 7 of an SF 153).

(7) Date of the receiving account transaction. This field is limited to six digits. Corresponds to the date entered in Block 5 of an SF 153.

(8) Transaction number of receiving account. This field is limited to six digits. Corresponds to the number entered in Block 6 of an SF 153.

(9) Total lines. This field is limited to four digits. Enter the total lines of material contained on the SF

d. **Explanation for Format Line 3 Text Entries**:

(1) ET/R3 -- "ET" is the compu ter flag for electrical transaction, "R" indicates receipt, and "3" represents the format line number.

(2) REMARKS. Used only to identify recipients of SAS/TPC material.

e. **EXAMPLE 3: Receipt ETR Message in JANAP-128 Format:**

```
RTTUZYUW RUHJWUA4111 2752325 UUUU -SUU.                          (R
ZNR UUUUU
R 010245Z OCT 96 ZYB
FM USS BARRY
TO DCMS WASHINGTON DC
   CMIO NORFOLK VA//CMIO//                                       (R
BT
UNCLAS // N02283 //
SUBJ: COMSEC MATERIAL ETR
ET/R1/078002/960920/601035/380092/960930/600034/1/10
(1)(2) (3)   (4)   (5)   (6)   (7)   (8) (9)(10)
ET/R1/880093/960918/606178/380092/960930/600037/5/25
ET/R3/RECEIPT ACKNOWLEDGED FOR NSA TN 606178 OF 960918 BY MR JOHN
ET/R3/J. JONES, GS13, 123 -45-6789 AND LTJG WILLIAM W. WILLIAMS,
ET/R3/USN, 987 -65-4321.
(11)  [ -  -  -  -  -  -  - (12)  -  -  -  -  -  -  -  -  -]
```

(1) Computer flag for electrical transaction.
(2) "R" for Receipt and "1" for format line number.
(3) CMS account number of the transferring command.
(4) Date of report (i.e., date on the SF 153).
(5) Transaction number of the transferring account.
(6) CMS account number of the recipient.
(7) Date of receipt.
(8) Transaction number of the receiving account.
(9) Total lines of material received.
(10) Total quantity of material received.

f. **EXAMPLE 4: Receipt ETR Formatted by ANCRS for Transmission via CARS:**

```
ET/R1/078002/960920/601035/380092/960930/600034/1/10
(1)(2) (3)    (4)    (5)    (6)    (7)    (8)  (9)(10)
```

NOTE: This CARS ETR receipts for the CMIO Norfolk shipment only. If SAS/TPC material is receipted for via a CARS ETR, the "ET/R3/" line must be manually formatted and will contain the name and SSN of the individuals receipting for the material.

1. Purpose. Transfer/Receipt ETR (also referred to as the "S" report) is a combined report used to report to DCMS (and the originator of the shipment) both the receipt and transfer of AL 1 or AL 2 COMSEC material between DON CMS accounts (except for accounts 078000, 078002, 360109; and DIRNSA accounts 880093 and 880099).

NOTE: Shipments received from the six accounts listed above must be receipted for using the Receipt ETR procedures contained in Tab 1. The above accounts provide DCMS with an advance notice (including short title identification) of material shipped to DON CMS accounts. Thus, the short title information is already in the DCMS database (in a pending file) awaiting receipt acknowledgement by the recipient via a Receipt ETR.

2. Policy:

a. A SF 153 Transfer Report must be prepared by the transferring command and enclosed in the shipment.

b. The Transfer/Receipt ETR must be prepared and transmitted by the recipient of a shipment within 96 hours of receiving a shipment. (**NOTE**: See timeframe for reporting receipt in Article 742.b.)

3. Transfer/Receipt ETR Format: The Transfer Receipt ETR consists of two format lines:

a. "S1": Contains receipt data identical to a Receipt ETR.

b. "S2": This line contains the identification of the short title(s) of AL 1 or AL 2 material transferred from the originator of the shipment that are receipted for in the "S1" format line.

4. Reporting/Documentation Requirements: The method used to transmit the Transfer/Receipt ETR (i.e., CARS or message) will determine how documentation requirements (i.e., handling of the SF 153) are fulfilled. The following options are provided for

(2) Attach a copy of the Transfer/Receipt ETR to your copy of the completed SF 153 and file them in the Chronological File. Annotate on the transfer/Receipt ETR that it was transmitted via CARS on YYMMDD (e.g., 960815).

NOTE: If a Transfer/Receipt ETR submitted via CARS receipts for SAS/TPC material transferred between DON accounts, the completed SF 153 must be returned to the originator.

b. ETR Sent via Message:

(1) Include the originator of the shipment as an info addressee on the Transfer/Receipt ETR message.

(2) Complete the SF 153 and attach a copy of the Transfer/Receipt ETR message and file them in the Chronological File.

NOTE: The Chronological File of the shipment originator must contain the completed SF 153 or a copy of the Transfer/ Receipt ETR message attached to their copy of the SF 153 as verification of r eceipt.

NOTE: Do not forward copies of corresponding SF 153s to DCMS for Transfer/Receipt ETRs submitted via CARS or message.

5. Discrepancies:

a. Discrepancies discovered upon receiving/opening a shipment such as missing/extra material, wrong serial number(s), pagecheck errors, damaged inner packages, packages showing evidence of tampering, and other discrepancies noted in the material itself or in the shipping containers/methods are **not** to be reported in an ETR.

b. Report discrepancies in accordan ce with the guidance contained in Article 742.c.

7. Transfer/Receipt ETR Format:

a. This Tab will show a sample Transfer/Receipt ETR in message format and then show the same ETR as it would be formatted automatically by ANCRS for transmission via CARS.

b. After the sample Transfer/Receipt ETR formatted by ANCRS will be an explanation for the data fields in each of the format lines. The explanations pertain to data fields formatted by ANCRS and to those that are manually prepared.

c. Annex W paragraph 9 contains the procedures for the message preamble/heading for ETRs submitted in message format. Mandatory elements in the example message headings in this Tab are bolded and underlined for emphasis.

d. Format line numbers an d numbers enclosed in parentheses under the ETR data fields in the examples that follow are for explanation purposes only. They must not be used in ETRs that are transmitted via CARS or in message format.

8. Transfer/Receipt ETR Examples and Formatting Explanations:

a. EXAMPLE 1: Sample Format for a Transfer/Receipt ETR Message in ACP 126 Format:

RTT**U****ZYUW** RULYDEA 3280 1621906-UUUU-SUU.
ZNR UUUUU
R 011907Z JUN 96 ZYB
FM USS LITTLE ROCK
TO DCMS WASHINGTON DC//30//
INFO (PLA OF COMMAND THAT TRANSFERRED THE MATERIAL)
BT
UNCLAS // **N02283**//
SUBJ: COMSEC MATERIAL ETR

(FORMAT LINE 1)

ET/S1/999999/YYMMDD/999999/999999/YYMMDD/999999/9999/99999

b. EXAMPLE 2: Sample Format for a Transfer/Receipt ETR as Formatted by ANCRS for Transmission via CARS:

(FORMAT LINE 1)

```
ET/S1/999999/YYMMDD/999999/999999/YYMMDD/999999/9999/99999
(1)(2) (3)    (4)    (5)    (6)    (7)    (8)   (9)   (10)
```

(FORMAT LINE 2)

```
ET/S2/XXXXXX/XXXXX/999999/XXXXXX/XXXXXXXXXXXX/?/9/99999/999999
 (11) [- - - - - - - - - (12)  - - - - - - - - -](13)(14)  (15)
```

c. Explanation for Format Line 1 Test Entries:

(1) ET/ -- "ET" is the computer flag that stands for electrical transaction.

(2) S1/ -- "S" indicates a combined Transfer/Receipt report and "1" represents the format line number. (**NOTE:** The data fields in this line are formatted the same as a receipt ETR in Tab 1.)

NOTE: SF 153 block number references cited below are keyed to the latest SF 153 form (Rev. 9/88).

(3) CMS account number of the command that transferred the material. This field is limited to six digits. Corresponds to the account number in Block 2 of an SF 153.

(4) Date of report. This f ield is limited to six digits. Corresponds to the date entered in Block 3 of an SF 153 (e.g., 960824).

(5) Transaction number of the originating command. This field is limited to six digits. Corresponds to the number entered in Block 4 of an SF 153. (**NOTE**: If the material is from DIRNSA,

(7) Date of the receiving account transaction. This field is limited to six digits. Corresponds to the date entered in Block 5 of an SF 153.

(8) Transaction number of receiving account. This field is limited to six digits. Corresponds to the number entered in Block 6 of an SF 153.

(9) Total lines. This field is limited to four digits. Enter the total lines of material contained on the SF 153. If the total lines are less than four digits, do not add zeros to the front of the number (e.g., 28 line items would be entered as: "/28/").

(10) Total quantity. This field is limited to five digits. Enter the total quantity of material contained on the SF 153. If the total quantity is less than five digits, do not add zeros to the front of the number (e.g., 127 items would be entered as: "/127").

d. Explanation for Format Line 2 Text Entries:

(11) ET/S2 -- "ET" is the computer flag for electrical transaction, "S" indicates a combined Transfer/Receipt report and the "2" represents the format line number. Format line 2 contains short title information of the material transferred to an account. Multiple format line 2s are permitted and each must start on a separate line and begin with "ET/S2/".

(12) Short title of the material transferred. This field is limited to 41 characters including the slashes (/) and question marks (?). (**NOTE:** Annex W paragraph 7 contains the formatting requirements for listing short title information.

(13) AL code (1 or 2) of the short title.

(14) Quantity of the short title. This field is limited to five digits. If the quantity is less than five digits, do not add zeros to the front of this number (e.g., a quantity of 43 would be entered as: "/43/").

automatically count off the remaining numbers based on the number entered in the quantity field.

2. If you received more than one copy and the accounting numbers are not in consecutive order, each item must be listed on a separate format line 2 (ET/S2/).

3. Enter a question mark (?) in this field for AL 2 material (accountable by quantity only).

e. EXAMPLE 3: Transfer/Receipt ETR Message:

RT**T**U**ZYUW** RUHPDEA2504 1532218-UUUU- **SUU**
ZNR UUUUU
R 032147Z JUN 96 ZYB
FM USS BARRY
TO DCMS WASHINGTON DC//30//
INFO 100 PALMS SIERRA NEVADA TX//CMS//
BT
UNCLAS // **N02283**//
SUBJ: COMSEC MATERIAL ETR
ET/S1/369012/960520/600047/380092/960602/600035/2/24
(1)(2) (3) (4) (5) (6) (7) (8 (9)(10)
ET/S2/USKAT/?/4440/CZ/?/?/1/16/4888
(11) [- - -(12)- - - -](13)(14)(15)
ET/S2/USKAK/?/6789/DE/?/?/2/8/?

(1) Computer flag for electrical transaction.
(2) "S" for Transfer/Receipt and "2" for format line number.
(3) CMS account number of the transferring command.
(4) Date of report (i.e., date on the SF 153).
(5) Transaction number of transferring account.
(6) CMS account number of the recipient.
(7) Date of receipt.
(8) Transaction number of the receiving account.
(9) Total lines of material received.

(13) AL code (1 or 2) of the short title.
(14) Quantity of the short title.
(15) Accounting number, or lowest accounting number, of the short title. For **AL 2** material, insert a "?" in this field as shown in the short title "USKAK 6789."

f. EXAMPLE 4: Transfer/Receipt ETR Formatted by ANCRS for Transmission via CARS:

```
ET/S1/369012/960520/600047/380092/960602/600035/2/24
(1)(2) (3)    (4)    (5)    (6)    (7)    (8)  (9)(10)
ET/S2/USKAT/?/4440/CZ/?/?/1/16/4888
(11) [-------(12)-------](13)(14)(15)
ET/S2/USKAK/?/6789/DE/?/?/2/8/?
```

ANNEX X

REPORTING PAGECHECK OR OTHER DISCREPANCIES IN COMSEC MATERIAL/RELATED DEVICES AND CCI

1. **Purpose:** This Annex prescribes actions required when discrepancies are noted during pagechecks or verification for completeness of the following:

a. COMSEC keying material marked CRYPTO.

b. COMSEC manuals and publications.

c. Classified COMSEC equipments and related devices (includes CCIs).

2. **Using the Discrepancy Reporting Legend**:

a. The categories of COMSEC material that a discrepancy is applicable to are identified as follows:

K:	Keymat marked "CRYPTO".
CM/A:	Classified COMSEC -Related Manuals/Publications.
CA:	Classified Amendments.
UM/A:	Unclassi fied COMSEC -Related Manuals/Publications and Amendments
E:	Classified COMSEC Equipment (**not** designated CCI).
R:	Related Devices (**not** designated CCI).
CCI:	CCI Equipment and Related Devices

b. The above letters will appear in parentheses before each type of discrepancy in paragraph 3. Under the type of discrepancy will be the required action(s).

3. **Discrepancies and Required Action:**

(K) Pages or segments discovered missing upon initial receipt pagecheck.

Report IAW Chapter 9. If r eplacement material required,

DCMS//30// and CMIO must be action addressees.

NOTE: Do not pagecheck keymat sealed in canisters.

(K) Pages or segments discovered missing on occasions other than initial receipt pagecheck.

Report IAW Chapter 9. If replacement material is required, DCMS//30// and CMIO must be action addressees.

ANNEX X

REPORTING PAGECHECK OR OTHER DISCREPANCIES IN COMSEC MATERIAL/RELATED DEVICES AND CCI

(K) Duplicate pages or segments .

Retain duplicate pages or segments. Notify DIRNSA//Y13//, INFO DCMS//30// and controlling authority.

(K) Defective keying material .

Report defect to DIRNSA//Y13//, INFO DCMS//30//, CMIO, and controlling authority. Retain defective keying material until disposition instructions are received from DIRNSA. If replacement material is required, DCMS and CMIO must be action addressees.

(K) Pages or segments misnumbered and/or out of sequence . Resequencing of p ages is possible.

Report discrepancy to DIRNSA//Y13//, INFO DCMS//30//, and controlling authority. Resequence pages or segments.

(K) Pages or segments out of sequence . **NOT** possible to

resequence pages.

Report discrepancy to DIRNSA//Y13//, INFO DCMS//30//, CMIO, and controlling authority. Retain defective keying material until disposition instructions are received from DIRNSA. If replacement is required, DCMS//30// and CMIO must be action addressees.

(CM/A) Pages discovered missing or misprinted upon initial receipt .

Report discrepancy to originator, INFO DCMS//30// and CMIO. If replacement material is required, DCMS and CMIO must be action addressees.

(CM/A) Pages discovered missing on occasions other initial receipt pagecheck .

Report IAW Chapter 9. If replacement material required, DCMS//30// and CMIO must be action addressees.

ANNEX X

REPORTING PAGECHECK OR OTHER DISCREPANCIES IN COMSEC MATERIAL/RELATED DEVICES AND CCI

(CM/A) "Unclassified" pages discovered missing on occasions other than initial pagecheck .

Report to DCMS//30//, INFO CMIO. If replacement material required, DCMS//30// and CMIO must be action addressees.

(CM/A) Page(s) duplicated .

Report discrepancy to originator, INFO DCMS//30//. Retain page(s) and await disposition instructions.

(CM/A) Pages misnumbered and/or out of sequence; resequencing is possible .

Report discrepancy to originator, INFO DCMS//30// and resequence pages.

(CM/A) Pages misnumbered and/or out of sequence; NOT possible to resequence .

Report discrepancy to originator, INFO DCMS//30// and CMIO. If replacement material required, DCMS and CMIO must be action addressees. Retain defective material until disposition instructions are received from originator of material.

(CM/A) Technical data is incorrect or missing, or a preparation or format error is discovered .

Report discrepancy to originator, INFO DCMS//30//. Retain defective material until disposition instructions are received from originator of material.

(UM/A) All discrepancies .

Report IAW Chapter 10.

ANNEX X

REPORTING PAGECHECK OR OTHER DISCREPANCIES IN COMSEC MATERIAL/RELATED DEVICES AND CCI

(E/R/CCI) Component(s) discovered missing upon initial receipt .

Report missing component(s) to DCMS//20/30//, INFO CMIO or originator of shipment. If replacement required, originator of shipment must be action addressee.

(E/R/CCI) Component(s) discovered missing when equipment/device checked on occasion other than initial receipt .

Report IAW Chapter 9. Request replacement component(s) IAW Chapter 6.

(E/R/CCI) Defective equipment/device.

Attempt to have qualified technician repair locally. If unable to repair locally, contact CRF. (**NOTE**: Marine Corps elements contact supporting Electronics Maintenance Support Company (ELMACO) or Force Logistics Support Cryptographic Facility (FLSCF).

ANNEX Y
MINIMUM PAGECHECK REQUIREMENTS FOR COMSEC MATERIAL

Type of Material	Upon Initial Receipt	After Entry of Amend which changes pages	Upon Installation Modification	During CMS Account Inventories	During Watch Inventories	Prior to transfer to new account	Upon Destruction
	These Pagecheck Requirements do NOT apply to keying Material packaged in canisters						
Unsealed Keying Material	Yes	N/A	N/A	Yes	Yes	Yes	Yes
Resealed Keying Material	N/A	N/A	N/A	During F.C. Semi-annual keymat and combined Inventory	N/A	Yes	Yes
Unsealed Maintenance and Operating Manuals	Yes	Yes: by person entering & by person verifying entry	N/A	During F.C. inventory of of equip/pubs & combined Inventories	N/A	Yes	Yes
All Unsealed Amendments	Yes	Yes: by person entering & by person verifying entry	N/A	During F.C. inventory of of equip/pubs & combined Inventories	Yes	Yes	Yes
Unsealed Amendment Residue	N/A	Yes: by person entering & by person verifying entry	N/A	N/A	N/A	N/A	Yes
Maintenance and Repair (PWB or "Q") Kits	Yes (All Components) (See Note 1)	N/A	Yes (Classified Components Only)	During F.C. Inv of equip/pubs & comb. invs (classified comp-onents only)	N/A	Yes (All Components)	Yes
Equipment	Yes (Upon Uncrating)	N/A	N/A	During F.C. inventory of of equip/pubs & combined Inventories	Yes	Yes	Yes
Mandatory Modification NSA/NAVY		N/A	N/A		N/A	Yes	N/A

Note 1: Maintenance personnel must inventory all components upon Initial local custody receipt and upon return of repair kits

ANNEX Z

CMS RUNNING INVENTORY (R/I)

CONFIDENTIAL (When filled in)

RUNNING INVENTORY (R/I) OF COMSEC MATERIAL

SHORT TITLE OF MATERIAL	QTY	ACCOUNTING NUMBERS	AL CODE	FINAL DISPOSITION

Classified By: CMS 1. Removed from R/I file on _____.

Declassify on: Originating Agency's Determination Required.

_____ Page No. ____

(Command Title and Account Number)

CONFIDENTIAL (When filled in)

ANNEX Z
CMS RUNNING INVENTORY (R/I)

1. **Purpose:** The CMS Running Inventory (R/I) is used to record all AL 1 through AL 4 COMSEC material held by a CMS or Local Holder (LH) account.

2. **Preparing the Running Inventory:** The following procedures apply for entering COMSEC material on the running inventory and are applicable for both manual and ADP -prepared inventories.

NOTE: Accounts using the ANCRS program must comply with the procedures in the ANCRS documentation package and Article 718 (for printout frequency and retention requirements.

a. **Short Title (Column 1)**: List short titles in alphanumeric order. The short titles of unentered AL 1, AL 2, or AL 4 amendments, corrections to amendments, or modifications to equipment, must be listed in sequence directly beneath the short title of the basic manual or equipment.

NOTE: For short titles superseded on a monthly basis, it is strongly recommended that at least one page per short title be used. For short titles superseded more frequently than once a month, more than one page should be used. This practice will preclude frequent retyping of these pages because of frequent supersession.

b. **Quantity (Column 2):** List the quantity held for each short title.

c. **Accounting (Serial/Register) Numbers (Column 3):**

(1) Multiple copies of an edition of keying material having sequential (uninterrupted) accounting (serial/register) numbers may be listed as a single line entry.

(2) Equipment and manuals having accounting (serial/register) numbers should be listed individually, one accounting number to a line. This provides for an accurate record of disposition or identification of amendment/modification data.

(3) AL 2 and AL 4 keying material may be listed on a single consolidated line entry since they are accountable by quantity only.

ANNEX Z

CMS RUNNING INVENTORY (R/I)

d. **Accountability Legend (AL) Codes (Column 4):** Enter the appropriate AL code for each short title, including each unentered amendment or modification.

3. **Deletions from Running Inventory:** Deletions from the running inventory usually result from destruction of material. Less frequently, deletions are required because material has been transferred or lost. Short title entries must be deleted from the running inventory in accordance with the following procedures:

a. **Line Outs**: When an entire line entry is being deleted, only the information in columns 1 through 4 should be lined out.

b. **Disposition (Column 5)**: If the item deleted has been transferred, lost, or destroyed, and the disposition reported to DCMS, annotate the transaction number of the applicable DCMS COR Reportable accounting report. If item deleted was destroyed, and destruction was not reported to DCMS (i.e., destruction report forwarding was not directed by DCMS), insert the date the material was destroyed in YYMMDD format in this column. (**NOTE**: ANCRS users will substitute local TN for date material was destroyed.)

NOTE: This column may be used for other remarks as well as disposition.

4. **Command Title and CMS Account Number**: The command title and CMS account number is required on the first page only.

5. **Page Numbering:** When multiple pages are required for listing material holdings, each page will be numbered sequentially.

ANNEX AA
COMPLETING DCMS-GENERATED SF 153 INVENTORY REPORTS (R

1. **Purpose:** This Annex delineates procedures for completing the DCMS generated SF-153 Inventory.

2. **Obtaining the Inventory:**

a. Each CMS account command will automatica lly receive their DCMS **Fixed-Cycle** (FC) Inventory.

b. SPECIAL inventories must be requested. See Article 766 for details.

c. Accounts that have chosen electronic media (i.e., CARS) as their preference for receiving information from DCMS will find their inventory in their CARS mailbox NLT the third day of their FC inventory month. Accounts electing "hard copy" will have their FC inventory mailed to them the first week of their FC inventory month.

3. **Verification of Information on Inventory Procedural Check-Off List:**

a. When conducting the first FC inventory of the CY or a Combined Inventory (CI), the CMS Custodian (or Alternate) must verify and/or correct all the information contained on the check-off list and obtain all required signatures. The Procedural Check-Off List must be returned to DCMS, along with the completed FC or Combined Inventory.

(1) Do not list as local holders those units which are an integral part of the CMS account command (e.g., CIC, Radio Control, etc.).

(2) If your command has no local holder, annotate the Procedural Check-Off List to that effect.

b. When a DCMS-generated FC Inventory is used solely as a SPECIAL Inventory, the Custodian (or Alternate) is only required to obtain applicable signatures since the inventory is retained locally and **not** returned to DCMS.

4. **Inventory Limitations/Authorized Adjustments to Preprinted Report Heading Information on FC and Combined Inventory Procedural Check-Off Lists:**

a. Original copies : FC and Combined Inventories must be completed only through the preprinted TN on the Procedural Check-Off List. The original copies of these inventories must be returned to DCMS within 60 days of the date in block 3 of the SF-153 for reconciliation. (NOTE: Do not make adjustments pertaining to transactions after the preprinted TN on the Procedural Check-Off List).

ANNEX AA

COMPLETING DCMS-GENERATED SF 153 INVENTORY REPORTS

b. When using a FC Inventory as a Combined Inventory, check the applicable box on the Procedural Check-Off List. (R

c. Working copies : Working copies (copies other than the original) are to be retained at the account command. Commands may adjust the preprinted TN and date on their working copy of the FC or Combined Inventory for the purpose of conducting the inventory through the most current TN. Adjusted working copies must not be returned to DCMS for processing but must be retained at the command in accordance with Annex T.

5. **Authorized Adjustments to Preprinted Report Heading Information on SPECIAL Inventory Procedural Check-Off Lists :**

a. These inventories must be conducted through your most current TN. If the DCMS-generated SPECIAL Inventory will be used, adjust the preprinted TN and date on the Procedural Check-Off List to reflect the most current TN.

b. Do not return completed SPECIAL inventories to DCMS. Retain locally in accordance with Annex T.

6. **Use a Black-Ink, Ballpoint Pen :**

To adjust or line out entries on the original copy of your SF 153 Inventory, use a black-ink, ballpoint pen. This will ensure full readability of these adjustments by DCMS personnel who must process and reconcile your reports.

7. **How to Complete the DCMS-Generated SF 153 Inventory :**

The lineouts/adjustments discussed below are based on the TN shown on the Procedural Check-Off List of the DCMS-generated SF 153 Inventory. Therefore, since the preprinted TN shown on the Procedural Check-Off List of a FC or Combined Inventory may **not** be changed, lineouts and adjustments made on the pages of these inventories must reflect only that material on charge to the account as of the preprinted TN.

Material that is listed on the inventory but which has been transferred, destroyed, lost or otherwise disposed of must be deleted from the inventory. Complete line outs as follows:

a. When material is disposed of was transferred, destroyed, lost, or otherwise disposed of and when disposition was reported to DCMS.

ANNEX AA
COMPLETING DCMS-GENERATED SF 153 INVENTORY REPORTS

(1) If all copies of any short title listed on the inventory have been disposed of, line out the entire entry and insert the TN(s) of the applicable DCMS reportable accounting reports in the remarks column. **(Note the requirements in paragraph 10).**

(2) If only some of the copies of any AL 2 quantity accountable short title listed on the inventory have been disposed of, change the quantity of the item to reflect the quantity currently held and insert in the remarks column the TN(s) of the applicable DCMS reportable accounting report(s). **(Note the requirements in paragraph 10).**

(3) If only some of the copies of any AL 1 serial number accountable short title listed on the inventory have been disposed of, change only the quantity to reflect the quantity currently held and insert in the remarks column the accounting/serial number(s) of the copies disposed of, and TN(s) of the applicable DCMS reportable accounting report(s). **(Note the requirements in paragraph 9).** (R

b. When material listed on the inventory was destroyed, and destruction was not reported to DCMS (i.e., destruction report forwarding was not directed by DCMS), these instructions apply:

(1) If all copies of any short title listed on the inventory have been destroyed, line out the entire entry and insert the date material was destroyed in YYMMDD format in the remarks column.

(2) If only some of the copies of any AL 2 quantity accountable short title have been destroyed, change the quantity of the item to reflect the quantity currently held and the date the material was destroyed in YYMMDD format in the remarks column.

(3) If only some of the copies of any AL 1 serial number accountable short title have been destroyed, change the quantity to reflect the actual quantity currently held and insert in the remarks column the accounting/serial number(s) of the copies destroyed and the date material was destroyed in YYMMDD format. (R

NOTE: ANCRS Users will substitute local TN(s) for date material destroyed.

c. When all copies of any short title listed on the inventory are not identified as in-transit (IT) and account records indicate the material was never received, line out the entire entry and insert **"NEVER HELD"** in the remarks column.

ANNEX AA

COMPLETING DCMS-GENERATED SF 153 INVENTORY REPORTS

d. When material listed on the SF 153 is identified as being in-transit (IT) to the account, the in-transit remark is treated as follows:

(1) Material not received : If material identified as IT has not been received, leave the entire entry as originally printed to indicate that the material is still in transit and is not on charge to the account.

(2) Material received : If material identified as IT has been received, line out only the in-transit remarks and insert the receipt TN in the remarks column adjacent to the line entry.

NOTE: AL 4 material will only appear on a SF 153 if it is in-transit to the account or in-transit and pending destruction to the account (IT and PD). In either case, annotate the remarks column for AL 4 material with the receipt TN of the SF 153 Transfer report. Do not enter local destruction TNs, even if the material has been destroyed.

e. If material listed on the SF 153 is identified as pending destruction (PD), the pending-destruction remarks are treated as follows:

(1) Material not destroyed : If material identified as PD has not been destroyed, leave the entire line entry, including all pending destruction remarks as originally printed to indicate the material is still charged to the account.

(2) Material destroyed : If material identified as PD has been destroyed, line out the entire line entry (including the pending destruction remark) and follow those additional instructions outlined in paragraph 7.a or 7.b, as appropriate.

f. If material listed on the inventory is identified as **both** In-transit and Pending Destruction (IT and PD):

(1) If material identified as PD and IT has not been received, leave the line entry as is to indicate that the material is still in transit to the account.

(2) If material identified as PD and IT has been received, but has not been destroyed (because destruction is not yet authorized), line out the IT remark and insert the receipt TN above the lined out IT remark.

ANNEX AA

COMPLETING DCMS-GENERATED SF 153 INVENTORY REPORTS

(3) If material identified as PD and IT has been received and destroyed, line out the entire line entry, including the IT and PD remark, and insert the receipt TN above the lined out IT and PD remark.

g. Obsolete Material Retained by Special Authorization:

If DCMS or higher authority has granted special authorization to retain obsolete or superseded material beyond its normal destruction date (e.g., for purpose of an investigation), line out any preprinted remarks and cite the originator, message date-time-group or letter serial number, and date of the special authorization in the remarks column.

h. Adjusting TOTAL LINES/TOTAL QUANTITY:

The preprinted TOTAL LINES/TOTAL QUANTITY information at the end of the SF 153 need not be adjusted, regardless of whether or not line entries on the DCMS SF 153 were annotated.

i. Initials on Lineouts/Adjustment

All lineouts/adjustments/entries made on the SF 153 can be initialed by the CMS Custodian and/or alternate who conducted the inventory and by the qualified witness. The inclusion of initials for changes is at the discretion of the account command.

8. **How to Add Material to the DCMS-Generated FC or Combined SF 153 Inventory:**

When conducting a FC or Combined Inventory, add only that material to the inventory that was received prior to the preprinted TN in the Procedural Check-Off List. Add material to this section of the inventory as follows:

a. Use additional SF 153s to add material to the DCMS-generated inventory. List or add **only** AL 1 and AL 2 material to this section.

b. In the **TO**

ANNEX AA

COMPLETING DCMS-GENERATED SF 153 INVENTORY REPORTS

c. The beginning line number on your first (or only) add-on sheet will pick up from the last SF 153 inventory page. For example, if the last line number on your DCMS-generated inventory is 162, the first line number on your add-on page will be 163. Even if an item is lined out (perhaps because it was "never held"), the line-numbering system will be unaffected. Using the previous example, if lines 158 through 162 are lined out as "never held," the first line number on the add-on sheet would still be 163.

9. **SF 153 Signature Requirements:**

a. When completed, the inventory must be signed by the Custodian and/or Alternate who conducted the inventory, by a qualified witness, and by the CO, OIC, SCMSRO. For an inventory which involves a Change of Custodian and/or Command, the Commanding Officer assuming command and/or the incoming Custodian must sign the inventory report. Signature of the Commanding Officer being relieved is optional.

b. Block 17 of the "last" page of the DCMS-generated inventory (i.e., not the last page of an add-on sheet) is reserved for the Commanding Officer's signature. The custodian and witness will add their signatures to Block 15 of this same page.

NOTE: In the absence of the Commanding Officer, the Executive Officer must sign the inventory as "Acting" Commanding Officer vice "By direction."

10. **What to Forward Along with Your Completed DCMS-Generated SF 153 FC and Combined Inventories:**

a. Forward the original DCMS-generated SF 153.

b. Forward a copy of your CMS TN log.

c. For each DCMS reportable TN annotated on the DCMS-generated SF 153, provide a copy of the associated SF 153 accounting report.

d. Do not submit copies of destruction reports unless specifically directed to do so by DCMS.

ANNEX AA

COMPLETING DCMS-GENERATED SF 153 INVENTORY REPORTS

11. **Preparing Your inventory Package For Mailing:**

Mark "CMS Inventory Report" on the inner envelope in bold letters. Include in the envelope only those documents identified in paragraph 10. This will ensure that your completed inventory is properly handled and routed within DCMS.

12. **Notify DCMS of Delays in Completing and Returning Your FC and Combined Inventories:**

If operational commitments or othe r unusual circumstances will preclude your being able to complete and return a FC or Combined Inventory to us, notify us by message. Your message must identify the SF 153 as a FC or Combined Inventory, the date of the reports preparation, the reason for the delay, and the anticipated date of completion and/or forwarding.

13. **Notice of Inventory Reconciliation:**

DCMS will accept for processing only SF 153 FC and Combined Inventories. All line outs, adjustments, and notations on these inventories will be researched and reconciled by DCMS Account Analysts.

a. Reconciliation may sometimes require the assistance of the account command; therefore, your prompt attention and response to our questions and requests information will be appreciated.

b. A Notices of Inventory Reconciliation will appear on Procedural Check-Off Lists (i.e., "Date of Last INV Recon:___"). This notice will reflect the date of the last SF 153 inventory reconciled for the account.

(1) This notice does **not** indicate that your account is error free.

(2) It means only that the information supplied on the inventory is consistent with the DCMS database as of the preparation date of that inventory.

ANNEX AB

LOCAL COMSEC MANAGEMENT DEVICE (LMD) SUITES

1. **Purpose**. To discuss the LMD suites, general management, and approved software application packages.

2. LMD suites (i.e., CPU, keyboard, monitor, and printer) are used to support the Navy Key Management System (NKDS). The following is a complete list of approved application packages for use on the LMD:

a. Word Perfect (V5.1 or V6.0)

b. Enable (V4.5)

c. MTF Editor (V4.0)

d. Tool Box (V1.9)

e. STU-III Management Program (STUMP) (V3.0A)

f. STU-III Key Ordering Software (V1.1)

g. ANCRS (V4.0)

h. UU-413 ASCII Encoding Software (V1.0)

i. PROCOMM Plus (V2.01)

j. DBASE IV (V1.5)

k. DBASE III

l. Form Tools (V3.0) Includes generation of logs and forms

m. Message Dissemination Utility (MDU) (V2.11C)

n. Message Traffic Viewer (MTV) (V3.5)

o. SACS Network Manager (SNM) (V1.0)

p. Lotus Smartsuite (Release 2)

q. DOS (V5.0)

NOTE: ANCRS version 4.1 is scheduled for release 4th quarter calendar year 1995 and is authorized for use upon release.

ANNEX AB

LOCAL COMSEC MANAGEMENT DEVICE (LMD) SUITES

3. The Joint Tactical Information Data System (JTIDS) Key Management Software versions 2.0, 2.01, 3.0 and, version 3.2 are approved. Using DOS version 5.0 is recommended when running these applications. The system must be rebooted before and after JTID software is run.

4. CD-ROM models that have been tested and approved for use with the LMD are: Sony CD-ROM Model CDU 625 version AA (used for K-Ware and Naval Warfare Publication (NWP) software) and Plextor DM-5028 external CD-ROM. Due to additional hardware requirements, refer all questions for CD-ROM to the LMD Trouble Desk.

5. Locally purchased laser printers are approved for use with the LMD; however, technical support may not be available for all models of non-standard print drives/hardware models.

6. Gateguard requests must be evaluated on an individual basis. Forward message requests to DCMS WASHINGTON DC//50//, Info COMSPAWARSYSCOM WASHINGTON DC//PD71M// and NRAD SAN DIEGO CA//87//.

7. Future software releases such as RBECS will be evaluated for use on the LMD as they are fielded. Custodians are advised not to use DOS V6.1 Utility (Doublespace) on the hard drive. Due to the large number of reported problems, recommend custodians running Windows (V3.1) not run ANCRS through Windows but as a stand-alone package.

8. LMD suites are intended for exclusive use of CMS personnel for automated management of COMSEC material. The NKMS is classified Secret. Once interface occurs with the DCMS system, all software, disks and associated electronic files held in the LMD are also Secret and can be declassified only per INFOSEC policies and procedures. In standalone mode, prior to interface with NKMS, ANCRS software that contains an account's running inventory is classified Confidential.

9. Accounts having LMDs with the requisite software and a STU-III terminal keyed at the Secret level, will comply with the following:

a. Maintain a running inventory and TN logs using ANCRS.

ANNEX AB

LOCAL COMSEC MANAGEMENT DEVICE (LMD) SUITES

b. Forward ETRs to DCMS via CARS or Autodin. mail paper copies of SF 153s only as a last resort (e.g., when not authorized to be sent via CARS, if to non-Navy accounts, or when Autodin is not available).

c. Access CARS FEP to print/download: (1) customized CMSRs; (2) SF 153 Fixed-Cycle Inventory and Special Inventory Reports; and (3) CMS Updates from CARS FEP bimonthly, within first five days of the month posted (e.g., CMS Updates disseminated February, April, June, August, October, December).

d. If you have changed your STU-III key, you most provide DCMS 50 Department with your new STU-III key ID prior to calling into the CARS FEP. Contact DCMS only when you physically change STU keys and not when you conduct an electronic rekey/update.

e. Replace VSTERM software with PROCOMM Plus software and load ANCRS 4.0. Refer to Annex F, titled COMSEC Automated Reporting System, for further details on communicating with DCMS via CARS.

11. Direct requests for waivers/exceptions to policy regarding LMD installations and/or LMD software configuration via message to DCMS WASHINGTON DC//50/TD//, Info COMSPAWARSYSCOM WASHINGTON DC//PD71M//, NRAD SAN DIEGO CA//87//, and ISIC/Chain of Command.

12 Direct all LMD technical questions or those relating to LMD installation/repair to the NKMS hot line at 1-800-656-7201. All questions relating to ANCRS/CARS, operations or procedures should be referred to DCMS (Code 50) at DSN: 764-0877 or commercial 202-764-0877/0704/0856.

ANNEX AC

ASSUMING THE DUTIES OF CMS CUSTODIAN

1. Introduction

a. If you've gotten this far, you're either curious or really are preparing to assume the duties of a CMS custodian. If the latter, you'll soon be managing the COMSEC material and equipment held by your command and keeping records of the whereabouts of each COMSEC material item. Think of yourself as the head accountant at a bank where you're responsible for accurately accounting for each dollar that comes into the bank and leaves it. That's really what being a CMS custodian is all about. It may not be easy, but it can be rewarding -- providing you don't lose any CMS "dollars."

b. The purpose of this section is to prepare you to intelligently assume the duties and responsibilities of CMS custodian. But you must also read and familiarize yourself with the following publications (ask the outgoing custodian to provide you with copies of these publications and to provide an overview them as well):

(1) CMS 1: The rules and regulations governing the operation of a CMS account are in this pub.

(2) CMS 6 and EKMS 702.01: If STU-III key and telephones are also managed and accounted for in the CMS account you are taking over, you will also need to read these publications. This is extremely important because the reporting requirements for STU-III key are unlike those for traditional COMSEC material.

c. By following the guidance in these publications carefully and fully, you will have no difficulty in ensuring that you meet the Navy's CMS objectives of SECURITY and ACCOUNTABILITY. CMS 1, CMS 6, and EKMS 702.01 (as applicable) are your most important management tools. Read and refer to these publication often. These pubs, attention to detail, and plain old-fashioned common sense will keep you out of trouble and in good standing with your Commanding Officer and Immediate Superior in the Chain of Command (ISIC).

d. Because most of you will be taking over an established account, this document is written on that basis and provides a very brief overview of the steps involved in assuming the job of primary custodian. This document also covers some of the key points, things you should be aware of *before* you assume the responsibilities for an account. You *must*, however, read CMS 1 (and CMS 6 and EKMS 702.01, as applicable) to get the details.

ANNEX AC

ASSUMING THE DUTIES OF CMS CUSTODIAN

2. Accounting for COMSEC Material

a. The material you will be working with is COMSEC material. Most of the time, you will see it referred to as CMS material, but the terms are used interchangeably. CMS material is unique in that each item of material, regardless of its use, is identified by a distinctly different short title, edition, and (in most cases) an accounting number.

b. Every piece of COMSEC material that is charged to your account is assigned an accounting legend code (ALC). (R There are three ALCs: 1, 2 and 4. These ALCs are very important because they tell you how to account for the material in your account. (See CMS 1, article 230, for ALC definitions).

3. Receipting for COMSEC Material

a. As a CMS custodian, you will routinely receive shipments of COMSEC material. Regardless of the ALC assigned to the material you receive, you will be required to report its receipt. You will report receipt using a SF 153 or an electronic receipt report.

b. The shipments you receive will originate from one or more of the following:

(1) The DCMS Vault

(2) COMSEC Material Issuing Office (CMIO) Norfolk

(3) Other Navy accounts

(4) Non-Navy accounts (e.g., Army, Air Force, the National Security Agency (NSA), NSA's Electronic Key Management Central Facility (EKMS CF), contractor accounts).

4. Inventorying COMSEC Material

a. As the CMS custodian, you are responsible for ensuring that you comply with the inventory completion and reporting requirements in CMS 1 (and CMS 6, as applicable).

b. In sum, the keying material holdings of each account must be inventoried twice each calendar year (CY). Equipment and manuals/publications must be inventoried once each CY.

ANNEX AC

ASSUMING THE DUTIES OF CMS CUSTODIAN

c. Each account automatically receives two DCMS-generated SF 153 Inventories each CY. These inventories are referred to as fixed-cycle inventories because they are generated and provided to accounts at predesignated 6-month intervals.

d. The account must complete and return the first inventory it receives in the CY. The second inventory, provided some 6 months later, is provided to assist the account in completing its second CY inventory of keying material. The results of this second inventory of keying material are to be retained locally (i.e., results are not reported to DCMS).

e. Accounts must also conduct inventories on these occasions: upon change of commanding officer, upon change of custodian, and just prior to disestablishing the account. Inventories conducted on these occasions are referred to as special inventories. A special inventory must be requested from DCMS. (R

5. Maintaining and Disseminating Material Status

a. In the interest of maintaining communications security and a high state of operational readiness, COMSEC material must never be used before it is authorized for use and must never be destroyed before it is authorized for destruction. In the world of CMS, we refer to a material's authorized use date as its effective date. A material's authorized destruction date is referred to as its supersession date. Both the effective and supersession dates of a COMSEC material item are referred to collectively as the material's status.

b. With the exception of COMSEC equipment, almost all COMSEC material is assigned effective and supersession dates. These effective and supersession dates are made available to commands in a monthly report called the Master COMSEC Material Status Report (MCMSR) or Customized COMSEC Material Status Report (C2MSR).

c. It is the custodian's responsibility to know the status of all COMSEC material charged to the account to ensure that it is used on time and destroyed on time. This responsibility holds true whether the material remains in the custodian's vault/safe or has been issued to local holders or users. When an item of COMSEC material has reached its assigned effective date, it is authorized for use. When an item of COMSEC material has reached it assigned supersession date, it is authorized for destruction.

ANNEX AC

ASSUMING THE DUTIES OF CMS CUSTODIAN

d. The custodian must advise local holder and user personnel of the status of materials issued to them. The custodian must be especially vigilant when it comes to maintaining material status because status changes occur with regular frequency. Status changes occur for routine reasons as well as for emergency reasons (e.g., the material is strongly suspected of having been compromised). Status changes are disseminated in general messages (ALCOMs, ALCOMLANTs, ALCOMPACs, etc.). Accordingly, before issuing materials for use or before

ANNEX AC

ASSUMING THE DUTIES OF CMS CUSTODIAN

c. SF 153s used to document the receipt of material requiring two-person integrity (TPI) and two-person control (TPC) requires two signatures: yours (or an alternate acting in your behalf) and a witness. The outgoing custodian should have advised you of any TPC materials that may be managed in the account and about TPC control procedures. If he/she didn't, ask.

d. All other SF 153s require only one alternate, yours or the alternate custodian acting in your behalf.

8. Pagechecking COMSEC Material

a. The pagechecking of COMSEC material is a very important part of assuming the duties of CMS custodian. Pagechecking ensures the completeness of COMSEC material.

b. The term "pagechecking" is another word for sight-verifying the segments of unsealed (i.e., not protectively packaged) keying material and the pages of unsealed classified publications. Pagechecking is also used to refer to the sight-verifying of various components of COMSEC equipment and related devices.

c. The importance of proper pagechecking cannot be overemphasized. For example, if a classified page from a manual is missing, you have a reportable COMSEC incident on your hands. Something you want to avoid! To minimize the occurrence of such incidents, ensure all unsealed keying material and unsealed classified publications are pagechecked during the change of custodian inventory and at the prescribed intervals thereafter. (Pagechecking policy (procedures, timeframes, items to be pagechecked) are outlined in CMS 1, article 757 and Annex Y. Procedures for reporting pagecheck discrepancies are outlined in CMS 1, Annex X).

9. The Mechanics of Assuming Duties as A Custodian: The Inventory

a. All COMSEC material holdings (i.e., ALC 1, 2 & 4) must be inventoried on the occasion of a change of custodian. (R

b. A SF 153 Inventory Report is used to officially document the change of custodian. (Inventory policies and procedures are outlined in CMS 1, article 766).

c. This inventory must be generated by DCMS. To obtain a DCMS-generated inventory, submit a message report to DCMS//30// and include the information outlined in CMS 1, article 766.d.(3)(6). (R

ANNEX AC
ASSUMING THE DUTIES OF CMS CUSTODIAN

d. In conducting the change of custodian inventory, you must either personally sight each copy of each item of material listed on the inventory or you must obtain written certification from the individuals holding the material (e.g., your users or local holders) that they do, in fact, have the material in their possession.

e. You must also pagecheck all the unsealed COMSEC materials as discussed above, or you may detail someone else to do it for you. If you don't personally conduct these required pagechecks, then others who assist you must certify in writing that they have indeed done them and must report discrepancies to you.

f. Accepting written certification from holders of material instead of personally sighting the material yourself should be resorted to only when it is not feasible for you to visit a remote user or local holder location, or if the material is held in spaces to which you normally would not have access because of special security requirements.

g. The written certification you accept under such circumstances should be a naval message, letter, or signed memo.

h. Once completed, the NKDS SF 153 Inventory should be verified (cross-compared) against the account's Running Inventory so that any differences can be cleared up before you assume custodial duties for the account.

i. Once you sign the inventory report, you are certifying the following to DCMS (the Navy's Central Office of Record for COMSEC material):

(1) that you have either seen each item of material listed on the inventory or that you have written certification from the holder(s) of the material that the items are in their possession; and,

(2) that you are taking responsibility for all the material listed on the inventory, as of the date of the inventory, until a new custodian assumes the duties and responsibilities.

10. Verify that Keying Material is Being Properly Maintained

a. Another important aspect of assuming the duties of primary custodian of an account is verifying that keying material in use is being properly maintained. We strongly recommend that you review the local records of destruction for

material currently being destroyed by users and local holders of the account to ensure the following:

(1) That two signatures appear for every segment of keying material that has been destroyed. (Ditto marks, connecting lines, etc., are prohibited.)

(2) That a date of destruction appears for every segment destroyed and the dates comply with the destruction timeframes in CMS 1. Again, no ditto marks, connecting lines, etc., are allowed.

(3) That the command is using appropriate local destruction records (i.e., locally prepared records contain all required fields of information). (See CMS 1, article 790 and example figures 7-1, 7-1, and 7-3.)

b. Improperly completed forms can constitute either a Practice Dangerous to Security (PDS) or a COMSEC Material Incident depending on the type and amount of information that has been omitted.

11. Review the Command's Last CMS Inspection Report

a. Finally, to get an idea of how well the account has been handled in the past and to ensure that you are not taking on any unfinished business, take a good look at the command's last CMS Inspection report or, time permitting, request an Advice and Assistance (A&A) Training Team Visit prior to taking over.

b. If there were any problems cited in the last CMS Inspection report, make sure they are either in the process of being squared away or that they have been resolved.

c. Remember, if you find anything wrong during the change custodian process, you have the right and responsibility to report the errors, COMSEC material incidents, or other problems to the Commanding Officer of the account. You should also make these errors or irregularities a matter of record at the time you accept the responsibility for the account, especially if you can't get them fully squared away before taking the job.

12. READ, READ, READ! Knowledge is your Best Defense!

a. As stated earlier in this document, the foregoing is a very brief overview of things to do or to be aware of before assuming the duties as CMS custodian of

ANNEX AC

ASSUMING THE DUTIES OF CMS CUSTODIAN

an existing account. You must read CMS 1 and, if applicable, CMS 6 and EKMS 702.1. Do not neglect to familiarize yourself with the COMSEC material incidents and Practices Dangerous to Security (PDS) sections in CMS 1 and CMS 6. Do nothing in a rush. Be thorough and pay attention to detail. There are no short-cuts in CMS.

b. If you ever feel confused or frightened about what to do don't panic! The worse thing you can do is N-O-T-H-I-N-G. Taking no action will only make matters worse. We're here for you. Start by calling your servicing A&A team or DCMS (Code 20 or 80). You'll find these phone numbers in CMS 1. We'll do everything we can to assist you and advise you. That's why we're here. GOOD LUCK!!!

CMS POLICY AND PROCEDURES FOR THE AN/CYZ-10 OR DATA TRANSFER DEVICE (DTD)

1. Purpose

To prescribe the minimum policies and procedures for the handling, safeguarding, and accounting of DTDs and related materials. These procedures are intended to provide maximum flexibility, yet ensure that proper security and accounting controls are in effect to preclude the loss of this material and the compromise of the information it protects.

This doctrine covers the use of the DTD as a common fill device and assumes the reader is familiar with DTD operation. The DTD User's Manual details DTD operation.

This Annex is divided into three parts: Part I contains the safeguarding and handling policy for the DTD, Part II provides definitions of unique terms used in Part I (unique terms are italicized where they first appear in Part I), and Part III provides limited guidance on DTD repair. More detailed guidance on repair and maintenance will be provided in a future amendment.

Procedures for operation of the DTD are contained in the DTD User's Manual (ON477340).

2.

The AN/CYZ-10 is the full keyboard version and the AN/CYZ-10A is the limited keyboard version of the DTD.

For compatibility with existing equipment, the DTD has a 6-pin I/O connector and will operate according to DS-101, DS-102, RS-232, and MIL-STD-188-114 interface specifications.

A fill device application program is provided with the DTD to perform functions comparable to those currently performed by the KYK-13, KYX-15A, and KOI-18. This software also allows the DTD to handle keys with lengths other than 128 bits.

The DTD is powered by a standard 9-volt battery, three 2/3 lithium batteries, or a rechargeable battery pack.

WARNING: The following battery types will **not** be used in the DTD: Mercury batteries nomenclated BA 1372/U and lithium batteries nomenclated BA 5372/U. Use of these batteries has proven extremely hazardous and has resulted in combustion.

4. DTD Capabilities

The DTD provides cryptographic security for the storage and transfer of all types of key and protective storage for related data (key tags, audit data, and application software).

The DTD is approved for processing all classification levels of key and data.

In addition to being used as a common fill device, the DTD will become an integral component of the Navy Key Management System (NKMS).

The functionality of the DTD is dependent on the application software which resides in it.

5. *Crypto Ignition Key* (CIK) Description

The DTD uses a CIK to control access to the cryptographic capabilities of the device. In general, when a CIK is inserted in the DTD and the DTD is powered on, the cryptographic capabilities of the DTD are unlocked to allow the input/output and handling of key and other information.

There are two types of CIKs: User and Supervisory. *User CIKs* allow the DTD operator to perform all the basic handling and distribution functions of the DTD. The *Supervisory CIK*

has all the privileges of the User CIK and additionally allows the *Supervisory User* access to all the DTD's functions, including the Utilities and Setup default applications.

In addition to controlling access based on supervisory versus user privileges, the DTD's CIKs can also be used to control access to key stored in the DTD's key storage database. The DTD's key storage database can be divided into compartments with access to the key in the different compartments granted only to users with specific CIKs.

6. DTD Keying

a. **Types of Key**. The DTD handles two types of key: DTD key and User key. DTD key is needed for the DTD's own internal use. The User key is key which is stored and transferred by the DTD for use by other cryptographic devices, equipment, and systems).

b. **DTD Key (or Internal Use Key)**:

(1) *Storage Key Encryption Key* (SKEK)[1] is used to store keys in the DTD's storage database in encrypted form to prevent exposure to the keys when the associated CIK is removed. SKEK is generated by the DTD when the DTD is initialized with the CIK. It is split and inaccessible when the CIK is removed, but recombined and accessible when the CIK is again inserted. When the DTD's key storage database is compartmented, there is a unique SKEK per compartment.

NOTE: Before reinitializing a CIK to create its new SKEK, ensure that the DTD is not storing keys protected by the CIK's current SKEK. Once the CIK is reinitialized, such keys cannot be recovered.

(2) *Transfer Key Encryption Key* (TrKEK) may be used in the DTD to output previously encrypted user key (key loaded into the DTD as encrypted key) in unencrypted form. The TrKEK may be filled into the DTD via hardcopy punched tape and loaded into the DTD via KOI-18, or it may be filled into the DTD in electronic form from another DTD or KOK-21 Key Processor (KP).

NOTE: **1.** When TrKEK is loaded into a DTD storing keys encrypted with that TrKEK, the keys are considered unencrypted when the CIK is inserted (**see paragraph 8 for effect on overall DTD classification**). To minimize DTD handling and safeguarding

[1] Also known as Local Key Encryption Key (LKEK).

requirements, do not load TrKEK into the DTD until the keys need to be decrypted for use.
2. To the extent possible, TrKEK should be pre-positioned or sent to the destination in a separate path from the DTD.

c. **Cryptoperiods**.

(1) DTD-generated SKEK has a one-year cryptoperiod.

(2) TrKEK has a three-month cryptoperiod which begins when the TrKEK is first used to encrypt key (its effective date). The TrKEK may be stored in the DTD for a maximum of six months before its effective date.

d. **Classification and ALC**.

(1) SKEK is classified according to the highest classification of key it secures in the DTD. DTD-generated SKEKs do not have an ALC since they are never handled outside the DTD.

(2) TrKEK is classified according to the highest classification of material it secures and is designated CRYPTO. It is assigned ALC 1.

7. <u>DTD & CIK Accounting Requirements & CIK Serial Number Assignment</u>

a. The **DTD** is accountable to DCMS in accordance with ALC 1.

b. The **CIK** is locally accountable to the CMS Custodian/ Supervisory User by assigned serial number. The policy for CIK serial number assignment follows.

c. The CIK serial number will be composed of the last four digits of the associated DTD serial number, followed by '01' for the CMS Custodian's Supervisory CIK, '02' for the Supervisory User's CIK, or '03' through '08' for the User CIKs.

8. <u>DTD Classification & Handling</u>

a. The DTD is unclassified CCI until:

(1) the DTD contains classified data on the *host side* (whether or not CIK is

inserted),[2]

or

(2) an associated CIK is inserted that can output classified (unencrypted) key from the DTD.

b. When only (1) is true, DTD assumes classification of data.

c. When only (2) is true, DTD assumes classification of key.

d. When both (1) and (2) are true, the DTD assumes the higher classification.

e. When the DTD contains key previously encrypted in a TrKEK (loaded into the DTD as encrypted key), and users are denied access to that TrKEK, DTD is UNCLAS CCI (whether or not CIK is inserted) **or** DTD assumes classification of host side data, whichever is higher.

f. A classification tag must be attached to the DTD via the lanyard ring to indicate the handling required for the DTD when the CIK is not inserted.[3]

9. CIK Classification & Handling

a. The CIK is classified to the highest level of unencrypted key it can output from the DTD. The CIK will retain that classification until the key is zeroized from the DTD.

b. A CIK that can output only encrypted key from the DTD is unclassified, providing the TrKEK used to pre-encrypt the key is inaccessible to users.

c. A tag must be attached to the CIK (e.g., via chain) to identify the CIK's classification and serial number.

d. If a CIK fails to work, check the update count. If the update count in the DTD is higher than on the CIK, it means an unauthorized copy of the CIK has been used in the DTD and the key should be considered compromised. See paragraph 25 (Reportable COMSEC Incidents).

10. TPI Requirements

[2]The CIK does not control access to the data on the host side of the DTD. That data can be viewed without the CIK being inserted.

[3]Classification tags are available through the Federal/National Stock System; reference stock number 5810-01-393-2942 **and** part number ON 477366-1 in your requests.

a. *Classified CIKs* require TPI handling and storage. Classified CIKs are defined as CIKs that can be used to output classified (unencrypted) key **designated CRYPTO** from a DTD.

b. When authorized users will not be present, a classified CIK must be removed from the DTD and returned to TPI storage. Otherwise, both the CIK and DTD must be continually safeguarded according to TPI rules.

c. When TPI storage is limited, and it is necessary to store more than one classified CIK in a single TPI container, each CIK shall be individually wrapped in its own envelope, the signatures of two individual(s) authorized access recorded along the seams, and the seams taped shut with cellophane tape. Additionally, the CIK's classification and serial number shall be recorded on the outside of each envelope.

d. **Exceptions** to TPI Requirements:

(1) Mobile Users (e.g., USMC tactical units, Naval Special Warfare (SPECWAR) units, Naval Construction Battalion units, Explosive Ordnance Disposal (EOD) units, and Mobile Inshore Undersea Warfare Units (MIUWUs)) are exempt from TPI requirements only while operating in a tactical exercise or operational field environment.

(2) Aircraft: TPI is not required during the actual loading process in the aircraft, but TPI is required up to the flight line boundary (assuming DTD and CIK are being hand- carried simultaneously).

NOTE: **1**. Classified CIK(s) placed in an Air Crew comm box locked with TPI-approved combination locks fulfills TPI requirements. Consequently, one aircrew member may transport the locked comm box up to the flight line boundary.
2. Classified CIK(s) may be stored onboard the aircraft in a single-lock container while the aircraft is in a flight status.

(3) Flag (e.g., FLTCINC) communicators operationally deployed away from their primary headquarters are exempt from TPI requirements.

11. DTD/CIK Clearance & Access Requirements

a. A clearance is not required to externally view a CIK (Supervisory or User, classified or unclassified) or a DTD that contains no key or data. Neither is a clearance required to externally view an *unkeyed DTD* containing classified key designated CRYPTO or data.

b. Unrestricted access to a DTD or to a CIK associated with a DTD containing the

keying material requires a clearance equal to the level of handling required in paragraphs 8 and 9, respectively.

c. Unrestricted access to a DTD keyed with a classified CIK or to a classified CIK also requires participation in a formal cryptographic access program.

d. Unrestricted access to Supervisory CIKs must be limited to those who are authorized to perform all of the privileges allowed by the Supervisory CIK.

12. Storage of Key in the DTD

a. There is no limitation on the length of time that user key may be stored in the DTD. However, superseded key must be destroyed in accordance with paragraph 15 guidance.

b. Key must **not** be stored on the DTD host side. Report any known violations of this rule in accordance with paragraph 25.

13. Issue and Receipt of Key in DTD

a. Segments and/or entire editions of key of all classification levels may be issued in a DTD for further issue or use.

NOTE: When electronic key converted from keytape is loaded into the DTD, the keytape segments can be destroyed unless there is an operational requirement to retain them until superseded. If retained until superseded, they must be stored and accounted for in accordance with article 775e(2).

b. Operational requirements and logistical constraints will dictate how much key may be issued to users in a DTD. However, the amount issued must be kept to the minimum required to support operations so as to minimize the effects of a compromise. General guidelines for issue follow:

(1) Tactical units deploying in other than crisis/contingency situations should limit the number of segments loaded into the DTD to those required for the mission. Loading the DTD with key converted from keytape should be limited to those segments required while the unit is absent from COMSEC support. The exposed and/or prematurely extracted hard copy key segment(s) should be destroyed immediately after loading into the DTD, unless there is an operational requirement to retain them. If retained until superseded, they must be stored and accounted for in accordance with article 775e(2).

(2) Units deploying under realworld crisis/contingency scenarios may download the current edition plus the minimum amount of keying material necessary for the crisis scenario, up to a maximum of 90 days keying material, into a DTD. (Common FDs (i.e., KYK-13 and KYK-15) may not be used for this purpose.) Requests for extensions in excess of 90 days must be forwarded to DCMS WASHINGTON DC//20// (information copy to DIRNSA FT GEORGE G MEADE MD//V51//).

c. Recipients of key issued in a DTD will acknowledge receipt of the key by signing local custody documents. Minimum accounting information for the key will include:

(1) short title(s) or designator(s)

(2) classification

(3) date of generation and/or loading

(4) date of issue or transfer

(5) identity of issuers and recipient(s),

(6) controlling authority of key

(7) effective period of key

(8) serial numbers of DTD and associated CIK(s).

14. Local Inventory Requirements

a. For Other Than Watch Station Environment:

(1) Supervisory and User CIKs must be inventoried whenever the account conducts fixed-cycle or combined inventories. The CMS Custodian or Supervisory User may direct more frequent inventories. The window display of each DTD will also be verified to ensure that all CIKs (Supervisory and User) associated with each key in the DTD are visually verified.

(2) The CMS Custodian (or Alternate) must inventory Supervisory CIKs. The CMS Custodian may delegate the responsibility for inventorying User CIKs to the Supervisory User.

(3) The results of local inventories are reportable to the CMS Custodian.

b. For Watch Station Environment:

(1) The serial numbers of Supervisory CIKs, User CIKs, and DTDs will be visually verified whenever watch personnel change. The watch-to-watch inventory will serve as the record of inventory. There is no requirement to verify the presence of stored keys (using the DTD window display).

(2) The oncoming watch supervisor and a witness will inventory all Supervisory CIKs. The oncoming watch supervisor will designate appropriately cleared and authorized personnel to inventory User CIKs and DTDs.

(3) Inventory discrepancies will be reported immediately to the Supervisory User and the Custodian (or Alternate Custodian).

15. Destruction of Key in DTD

a. **Emergency Supersession Guidance for Custodians and Users**. Destroy/zeroize emergency superseded key as soon as possible and always within 12 hours of receipt of emergency supersession notification.[4]

b. **Routine Destruction Guidance for Users**.

(1) Regularly superseded key: Destroy/zeroize superseded key as soon as possible after the end of the cryptoperiod and always within 12 hours after the end of the cryptoperiod.

[4]The only authorized exceptions to this 12-hour destruction standard are in paragraphs 15b(1)(b) and 15b(1)(c).

The only authorized exceptions to this 12-hour destruction standard follow:

(a) Users need not remove classified CIKs from secure storage for the sole purpose of performing routine destruction of superseded segments. Users may postpone destruction of superseded segments until the entire edition is superseded or until the next use of the DTD, whichever occurs first. If superseded segments are retained until the edition is superseded, they must be destroyed no later than five working days after the month in which the edition is superseded.

(b) In the case of an extended holiday period (over 72 hours) or when special circumstances prevent compliance with the 12-hour standard (i.e., operational space not occupied),

d. **Documentation Requirements.** There is no requirement to document destruction of key in a DTD. DTD Audit trail reviews will serve to verify zeroization/destruction of key. See paragraph 17 for audit trail review requirements.

16. Transportation Guidance

a. Shipping the **DTD**

(1) **The DTD must always be shipped separately from its associated CIK(s) once the CIK(s) are initialized, whether or not the DTD contains keying material or host side data.**

(2) When the DTD contains no keying material and no classified host side data, transport using any of the means approved for UNCLAS CCI in article 535k.

(3) When the DTD contains only keying material (or keying material and unclassified host side data), and providing the corresponding CIK(s) are shipped separately, transport using any of the means approved for UNCLAS CCI in article 535k.

(4) When the DTD contains only classified host side data (or keying material and classified host side data), and providing the corresponding CIK(s) are shipped separately,
transport using any of the means approved in article 530c for the classification level of host side data.

b. Shipping the **CIK**

The CIK must be shipped separately from its associated DTD, using any of the means approved in article 530 for keying material of its classification. (See paragraph 9 of this Annex for CIK classification guidance.)

c. Hand Carrying the DTD **and** CIK(s)

Personnel authorized unrestricted access to a DTD and its corresponding CIK may be authorized to handcarry the DTD and CIK, as necessary. The DTD and corresponding CIK must be appropriately packaged and protected separately from each other (e.g., in a separate container or on the local command courier's person). TPI handling of the CIK will be required as follows:

(1) when the same local command couriers will be simultaneously handcarrying the DTD and classified CIK,

or

(2) when the local command couriers will be simultaneously handcarrying

the DTD and CIK and the TrKEK used to preencrypt the classified key (designated CRYPTO) in the DTD.

17. *Audit Trail Record* Review Requirements:

a. **General**. The DTD automatically records audit information on the actions performed by the DTD operators. Audit data can be reviewed in either the DTD itself, or by uploading and reviewing on a computer. The latter requires a special connector between the DTD and a computer and special computer software.

b. **Who Should Review**. The audit trail of each DTD storing keys must be reviewed by the Supervisory User (or other person designated by the local commander/officer-in-charge) using the Supervisory CIK. The audit trail reviewer should not be a primary user of the DTD, but should have enough knowledge of the authorized user(s) of that DTD and the keying material which the user handles to be able to detect anomalies in the audit trail.

Example anomaly: DTD audit trail reflects a key issue at 0300 when DTD is maintained in a comms facility operated part-time (i.e., from 0800 to 1600).

c. **Frequency of Review**. The audit trail must be reviewed at least once per month, although more frequent reviews are encouraged.

d. **Logging Reviews**. The designated reviewer will keep a log of all audit trails reviewed and indicate whether or not any anomalies were detected. These logs will assist the reviewer in tracking any trends or changes in audit information and alert the reviewer to potential security problems. Any potential security problems must be investigated to determine cause.

e. **Classification of Audit Trail Records**. When uploaded to a computer and/or stored to disk, DTD audit trail records are classified SECRET.

f. **Retention of Audit Trail Records and Audit Review Logs**.

(1) There is no requirement to retain audit trail records that have been reviewed and found free of anomalies. This applies to current audit trail data stored in the DTD and audit trail data uploaded to a computer and/or stored to disk.

(2) Audit review logs will be retained for at least two years.

18. DTD *Interface Flows*

a. **DTD as a common fill device**: Interface flows involving key/key tag and application software flows are not subject to computer security (system-high) rules. These flows are trusted to occur at their actual intended classification level. The fill device application program provided with the DTD is unclassified. The audit trail records created by the fill device application program are also unclassified until uploaded to a computer and/or stored to

b. **DTD use with an Automated Information System (AIS)**: Interface flows between the DTD and AIS's are **not** subject to computer security (system-high) rules. This includes any User Application Software (UAS) and audit data either uploaded or downloaded from a classified computer (e.g., LMD). For example, if UAS is downloaded from a LMD (Secret-high AIS) to the host side of a DTD, the DTD will **not** be classified on the basis of that connection/interface flow.

19. DTD Zeroization & Sanitization

a. When activated, the DTD's zeroization function will sanitize all data, destroy all stored key, and delete all CIKs from the DTD. (The zero function will not delete application software from the DTD, nor will it delete audit records from the DTD.)

b. Regardless of its handling requirement before zeroization, once the zeroization function is successfully completed, the DTD is UNCLASSIFIED CCI. The operator can only treat the DTD as zeroized if the display shows the "zeroization complete" message. If this message does not appear, a depleted battery may be the cause. Install a fresh battery and press the [ZERO] key the correct number of times to verify that the display message "zeroization complete" appears. If the message still does not appear, then it must be assumed that zeroization is not possible due to a malfunction. The battery must be removed from the DTD and the DTD must be protected according to its classification (see paragraph 8 for classification guidance) until it can be turned-in to a depot and repaired.

NOTE: There is a selective delete function on the DTD Utility menu which may be used for maintaining the accountability of the key. This delete function will not sanitize the DTD or reduce handling requirements of the CIK.

20. Supervisory User Responsibilities

a. Create CIKs and ensure that the number of CIKs created are kept to the minimum required to satisfy local operational requirements.

b. Ensure each CIK has a serial number to support its accountability in DTD audit trail records. The serial number will be created and assigned by the Supervisory User in strict accordance with paragraph 7c. When creating CIK serial numbers, the Supervisory User will ensure that the CIK serial number is unique from those for all other DTD CIKs associated with

the AIS or LMD which reviews his/her DTD's audit trail.

c. Establish procedures that ensure that an accurate determination can be made regarding which individual user(s) had access to a CIK at any given time.

d. Re-initialize CIKs at least annually and whenever key compromises occur.

e. Always store Supervisory CIKs separately from associated DTDs.

f. Ensure DTDs are examined for breaches in housing at least weekly.

g. If designated by local commander/officer-in-charge to be audit trail reviewer, review audit trail records as required by this document.

h. **Promptly** delete CIKs from DTDs that are suspected of having been copied (i.e., when CIK update count check reveals disparity between update count on DTD and update count on the CIK) and review audit records to determine whether CIK was copied and what unauthorized actions, if any, were performed with the copied CIK. If review results confirm that CIK was copied, notify CMS Custodian immediately so that a COMSEC incident report may be prepared and forwarded as required by paragraph 25.

i. Ensure a tag is attached to each CIK (e.g., via a chain) that minimally identifies the CIK's classification and serial number.

j. Ensure that a tag is attached to each DTD, via the lanyard ring, that indicates the classification of the DTD when its associated CIK is not inserted.

21. Operator Responsibilities

a. Whenever a CIK fails to work in its intended DTD, **promptly** notify the Supervisory User/CMS Custodian. He or she will check the update counts of the CIK and DTD to determine whether or not a review of audit trail records is required.

b. **Promptly** notify the Supervisory User/CMS Custodian of any DTDs storing key and CIKs that are not tagged as described under Supervisory User Responsibilities.

c. Examine DTDs for casing damage or cracks at least weekly.

d. Be familiar with the handling and safeguarding requirements of this doctrine and report all violations of same to the Supervisory User/CMS Custodian.

22. CMS Custodian Responsibilities for User Application Software

a. Ensure that only NSA cryptographically signed application software is installed in the DTD.

b. Maintain records of all UAS installed in each DTD charged to the account. These records will identify the DTD by serial number and the UAS installed in that DTD. In the event a DTD malfunctions, requiring turn-in to a CRF for replacement, these records will ensure that replacement DTDs (swap-out units) arrive with the required UAS installed.

23. Use of the DTD & STU-III for Tactical Over-the-Air Key Distribution

Use of the DTD and STU-III is the preferred, authorized method for transferring key for limited duration operations. The DTD and STU-III can be used to rekey units in the field who have telephone access as well as aircraft crews who may have landed at airports other than their own base. This can preclude carrying excessive amounts of paper material, especially if they plan an extensive number of days away from home base.

An NSA-approved adaptor/connector **must** be used to connect the DTD to the STU-III data port for purposes of passing key over STU-III secured point-to-point circuits.

Also see Chapter 11, article 1165e.

24. Emergency Protection

Follow the provisions of CMS 1 for the emergency protection of the materials in this document. To destroy the DTD beyond reuse during emergencies (e.g., impending site overrun and capture), where the alternative is possible compromise of the DTD and the key or data it protects, zeroize the DTD and smash with fire ax, hammer, or other heavy object.

25. Reportable COMSEC Incidents

a. The following incidents are specific to the DTD and are intended to supplement those general COMSEC incidents and practices dangerous to security (PDS) identified in CMS 1:

(1) Loss of a DTD or a CIK (reportable to the controlling authority for the key).

(2) Unauthorized copying of a valid CIK[8]

(3) Unauthorized access to a CIK or DTD.

(4) Storage of key on the host side of DTD.

(5) Loss of TEMPEST integrity because of failure to detect a breach in the DTD's housing.

b. Follow reporting guidance in CMS 1.

c. Compromise Recovery Actions for Lost CIK/Lost DTD.

(1) If a CIK is lost, promptly delete the lost CIK from its associated DTD and report the loss in accordance with CMS 1. In the report of loss, describe the degree of protection afforded the DTD when the CIK was first discovered missing. If the DTD was not in the protective custody of authorized user(s) when the CIK was lost, all key and host side data must be considered compromised.

(2) If a DTD is lost, promptly zeroize/destroy its associated CIK(s) and report the loss in accordance with CMS 1. In the report of loss, describe the degree of protection afforded all associated CIKs when the DTD was first discovered missing. If the DTD's associated CIK(s) were not lost/compromised, but remained under the protection required for their classification (e.g., TPI), the user key and TrKEK which were stored in the lost or compromised DTD need

[8]Compromise of key as a result of an adversary gaining unaccompanied access to and surreptitiously copying a valid CIK, which can be later used in the associated DTD **before** the original CIK is used.

not be superseded. Any classified host side data stored in the lost or compromised DTD must be considered compromised.

ANNEX AD - PART II

Definitions Unique to DTD Safeguarding & Handling Policy

Audit Trail Records - Chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event.

Classified CIK - A CIK that can be used to output classified (unencrypted) key designated CRYPTO from a DTD.

Crypto Ignition Key (CIK) - The information contained in a key storage device (KSD) that is used to electrically lock and unlock the secure mode of crypto equipment. When the KSD containing a CIK is inserted in the DTD and the DTD is powered on, the cryptographic capabilities of the DTD are unlocked to allow for the input/output and handling of key and other information. There are two types of DTD CIKs: User CIKs and Supervisory CIKs.[9]

Data Transfer Device (DTD or AN/CYZ-10) - The DTD provides cryptographic security for the storage and transfer of all types of key, and protective storage for related data (e.g., key tags and audit data) and other data depending on the application software in the DTD.

compartmented, there is a unique SKEK per compartment. The SKEK generated in the DTD has a one-year cryptoperiod.

Supervisory CIK - Has all the privileges of the User CIK and, in addition, allows the Supervisory User to perform utility functions such as loading application software and uploading and reviewing audit trails. Also see User CIK.

Supervisory User - Individual designated by CO/OIC to create CIKs, assign serial numbers to them, and to fulfill additional responsibilities for their handling and safeguarding (see paragraph 21). The Supervisory User and CMS Custodian may be one and the same.

Tactical Key - Traffic encryption key (TEK), key encryption key (KEK), or transmission security key (TSK) intended to secure information or data that is perishable, has low intelligence value (i.e., low national or international sensitivity), and is classified no higher than Secret.

Transfer Key Encryption Key (TrKEK) - Key used in the DTD to decrypt previously encrypted user key (loaded into the DTD as encrypted key) to enable the DTD to output user key in unencrypted form.

Unkeyed DTD - DTD which may or may not contain user key and/or TrKEK and does not have its associated CIK inserted. Also see Keyed DTD.

User CIK - Allows the DTD operator to perform all the basic key handling and distribution functions of the DTD. Also see Supervisory CIK.

User Key - Key which has been loaded into the DTD for storage and subsequent transfer to other cryptographic devices, equipment, or systems.

ANNEX AD - PART III

DTD Repair & Maintenance

Only limited maintenance may be performed on the DTD by users or other authorized personnel. Limited maintenance, as it applies to the DTD, is defined as hinge cover, keypad, and battery replacement. Personnel replacing these parts are not required to be Qualified Maintenance Technicians.

Further guidance will be published in Amendment 5.