From: Commander, Navy Reserve Forces Command

Subj: KEY MANAGEMENT INFRASTRUCTURE OPERATING ACCOUNT ADMINISTRATION AND MANAGEMENT PROCEDURES

Ref: (a) EKMS 1B  
(b) EKMS 3D  
(c) EKMS 5  
(d) EKMS for Commanding Officers Handbook  
(e) SECNAVINST M-5510.36  
(f) SECNAVINST 5510.30B

Encl: (1) Commander, Navy Reserve Forces Command Local Element Communication Security Administration and Management Procedures

1. Purpose. Provide policy and procedures for administration, management and handling of Communication Security (COMSEC) material within the Navy Reserve Force. This instruction is a complete revision and should be read in its entirety. This instruction is effective upon receipt.

2. Cancellation. COMNAVRESFORCOMINST 2280.1C.

3. Objective. Achieve uniform implementation of COMSEC policy and procedures for supported Local Element (LE) commands of Commander, Navy Reserve Forces Command (COMNAVRESFORCOM) Key Management Infrastructure (KMI) Operating System account 177015.

4. Applicability. This instruction, references (a) through (f) and enclosure (1) involves COMSEC administration, management, handling policy and procedures. These provisions apply to all commands and individuals requiring access to or the use of COMSEC material within KMI. All such personnel must be aware of non-compliance or deviation from the prescribed procedures that can jeopardize the security of the United States (U.S.) and could result in prosecution of the parties concerned under the espionage laws, Title 18. U.S.C., Sections 793, 794 and 798.

a. LE Commanding Officers (COs) are not authorized to appoint or assign contractor personnel as LE Custodians or as a COMSEC user.
Local Element
Communications Security Administration and Management Procedures
Foreword

The primary purpose of this publication is to provide detailed guidance to LE Custodians, so they are able to quickly and easily determine correct COMSEC material accounting and control procedures for all COMSEC material entrusted to them. This publication describes the minimum policies for issuing, accounting, handling, safeguarding, disposing of COMSEC material and the application of cryptographic/physical security measures to COMSEC material and facilities.

The policies in this publication are derived from those set forth in national and Navy COMSEC doctrine manuals. The guidance herein supplements, but in no way alters or amends the provisions of U.S. Navy Regulations, EKMS 1B, SECNAVINST 5510.36A and SECNAVINST 5510.30B.

This publication is effective upon receipt and available upon request.

Suggestions for amendments or improvement to this publication can be forward directly to the COMNAVRESFORCOM EKMS Team at cnrfc_ekmsteam@navy.mil.

Enclosure (1)
Electronic Key Management System Account Information

EKMS Account Number: 177015
Highest Classification Indicator: SECRET
Mailing Address:

COMNAVRESFORCOM
ATTN: EKMS Manager
1915 FORRESTAL DRIVE
BLDG NH-32
NORFOLK, VA 23551-4165

Days of Operation: Monday - Friday
Normal Duty Hours: 0730 - 1630

If you have a question or need assistance, do not hesitate to contact the COMNAVRESFORCOM EKMS Manager or EKMS team.

EKMS Immediate
Superior in Command: (757) 322-6649/DSN: 262-6649
EKMS Manager: (757) 322-6640/DSN: 262-6640
Alternate EKMS Manager: (757) 322-6638/DSN: 262-6638
EKMS Account Clerk: (757) 322-2144/DSN: 262-2144
COMNAVRESFORCOM SIPRNET Help: 1(757) 322-6666
Record of Changes

<table>
<thead>
<tr>
<th>CHANGE NUMBER IDENTIFICATION</th>
<th>DATE ENTERED (YMMDD)</th>
<th>ENTERED BY (SIGNATURE) RANK/RATE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table of Contents

Foreword .................................................. i
COMNAVRESFORCOM Electronic Key Management System Account Information .................................. ii
Record of Changes ........................................... iii

Table of Contents ........................................... iv

Chapter 1
- 1.1 Introduction to the Communications Security Material Control System
- 1.2 Communications Security Organization ...................... 1

Chapter 2
- 2.1 Establish a Local Element ................................... 4

Chapter 3
- 3.1 Local Element Administration ............................... 6
- 3.2 Local Element Folder ........................................ 6
- 3.3 Access List ................................................ 6
- 3.4 Visitor Register .............................................. 6
- 3.5 Combinations ................................................ 6
- 3.6 Communications Security Training ............................ 9
- 3.7 Commanding Officer Spot Checks ......................... 9
- 3.8 Destruction ................................................. 9
- 3.9 Emergency Action Plan .................................... 11

Chapter 4
- 4.1 Secure Terminal Equipment .................................. 13

Chapter 5
- 5.1 Forms .................................................. 15

Chapter 6
- 6.1 Request for Communications Security Material ............ 24
- 6.2 Shipping Communications Security Material ............... 24
- 6.3 Receiving and Opening Communications Security material Shipments ........................................ 25

Enclosure (1)
Chapter 1

1.1 Introduction to the Communications Security Material Control System. COMSEC material is 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 material used to ensure the authenticity of such communications. Examples of COMSEC material and U.S. Government transmissions is the use of the Non-Classified Internet Protocol Network, Secret Internet Protocol Network, KG-175D (TACLANE), Secure Telephone Equipment (STE) phone and Talon Solution (KOV-26).

a. The protection of vital and sensitive information moving over government communication 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 was established to distribute, control and safeguard COMSEC material. This system, which consists of production facilities, COMSEC Central Offices of Records, distribution facilities (i.e., depots) andEKMS accounts, is known collectively as the COMSEC Material Control System (CMCS).

b. COMSEC material is managed in EKMS accounts throughout the federal government to include departments and civil agencies as well as the civilian sector supporting the federal government. COMNAVRESFORCOM is assigned EKMS account number 177015.

1.2 Communications Security Organization. Mandated by National and Department of the Navy Policy, COMNAVRESFORCOM is responsible for accurately accounting for COMSEC material at all times for account 177015. The Commander appoints an EKMS Management Team to administer and manage his/her COMSEC program. Applying structured processes and procedures, the EKMS Management Team tracks each individual piece of COMSEC material from initial receipt to issuance and destruction. Figure 1.1 represents your COMSEC chain of command.

a. Immediate Superior in Command (ISIC). COMNAVRESFORCOM is responsible for the administrative oversight of all COMSEC matters for their subordinate commands.

b. Staff Communication Material System Responsibility Officer (SCMSRO). Per reference (a), the Commander elected to appoint a SCMSRO to assume personal responsibility for routine COMSEC matters. The EKMS Manager reports directly to the SCMSRO on all matters relating to COMSEC material management.
c. **Commanding Officer.** The CO is responsible for properly administering his/her COMSEC holdings, ensuring compliance with this instruction and established policies and procedures.

d. **EKMS Manager.** The EKMS Manager is appointed by the SCMSRO and designated, in writing, to manage his/her COMSEC program. The manager is responsible for all facets of COMSEC operations issuing policy and guidance to LEs while maintaining accountability of all COMSEC material issued at the command and LE level. The EKMS Manager shares these responsibilities with the EKMS Alternate Manager(s). All LE commands report directly to the EKMS Manager for matters relating to COMSEC material administration and management.

e. **Alternate EKMS Manager(s).** Alternate EKMS Manager(s) are designated in writing by the SCMSRO. Alternates are responsible for assisting the EKMS Manager in the performance of their duties and assuming the duties in their absence. The alternate shares equally with the EKMS Manager the responsibility for the proper administration and management of the EKMS account.

f. **EKMS Clerk.** An individual designated in writing by the SCMSRO, who assists the EKMS Manager and alternate(s) with routine administrative account matters. The account clerk assists in the daily operations of the account and manages routine matters.

g. **Local Element.** LEs are separate entities or remote commands that receive COMSEC support from the COMNAVRESFORCOM EKMS account. An entity is defined as internal to the command (i.e., SIPRNET Café, N3 Operations, Navy Operational Support Center (NAVOPTSPTCEN), etc). LE commands are directly accountable to the Commander for the proper administration and management of issued COMSEC material. LE Commands may receive tasking from their RCC while supporting tasking from COMNAVRESFORCOM; however, they are accountable to the Commander, reporting directly to the EKMS Manager for matters relating to COMSEC material administration and management.

h. **Witness.** A witness must be a qualified COMSEC user and is required to be familiar with applicable procedures of this publication and related command-issued directives. A witness should assist personnel in routine administrative tasks related to COMSEC material. An individual who witnesses an inventory,
destruction or any other COMSEC report is equally responsible for:

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

(2) Sighting all material inventoried when signing an inventory report.

(3) Sighting all material to be destroyed and witnessing the actual destruction of the material.

i. Reserve Component Commander (RCC). While RCCs do not manage COMSEC material, RCCs are administratively responsible for managing the accountability of COMSEC material. The RCC monitors, tracks and reports on EKMS compliance and deliverables to the EKMS Manager. The RCC will consolidate reports and gather the status of assigned tasking for further submission to the EKMS Manager. RCCs do not provide direction on the administration and management of LE COMSEC holdings.

Figure 1.1  COMSEC Chain of Command
2.1 Establish a Local Element. Prior to any command receiving COMSEC material from COMNAVRESFORCOM, they must first be established as an LE.

a. Memorandum of Understanding. An Memorandum of Understanding (MOU) must be exchanged between COMNAVRESFORCOM and the command requesting COMSEC support. The MOUS establishes the terms and conditions of support and requires the signature of the requesting command's CO and SCMSRO.

b. Facility Approval. As a condition outlined in the MOU, the requesting command must provide to the EKMS Manager a copy of the space certification to hold classified COMSEC material. This approval should be based upon a physical security inspection which determines whether or not the facility meets the physical safeguarding standards of EKMS 3C and EKMS 1B.

c. LE Custodian Appointment. LE Custodians must be designated in writing by the LE CO. Each LE must appoint, in writing, an LE Custodian and an Alternate LE Custodian to manage and administer his/her local COMSEC holdings. The appointment of two LE Custodians is for the destruction and inventory of COMSEC keying material. The following are the requirements of an LE Custodian:

(1) Be a responsible individual and qualified to perform his/her COMSEC duties.

(2) Be authorized in writing, to access COMSEC material by the current CO.

(3) Hold a final security clearance of SECRET or higher.

(4) Complete EKMS Managers Course (V-4C-0013) or EKMS Personnel Qualification Standards (PQS) Naval Education and Training (NAVEDTRA) 43462.

(5) Complete COMSEC User Acknowledgement Form.

(6) Hold an LE appointment letter.

Note 1: The EKMS account holder will forward all required forms, templates and briefs. Retain each form and letter in your LE folder, forward the original or copy, as applicable, to the parent EKMS account.

Enclosure (1)
Note 2: When forwarding documents via e-mail, attach a digital signature and when appropriate apply encryption. To ensure authenticity and integrity of your e-mail and any attachments. All emails should be sent to the following address: cnrfc_ekmsteam@navy.mil.
3.1 Local Element Administration. Attention to detail, focus and follow-up are the principal elements needed to properly administer and manage a command's COMSEC material holdings. Deviate from these principals significantly increase the risk of losing accountability of COMSEC material and required documents.

3.2 Local Element Folder. To facilitate the administration of various documents exchanged between you (the LE) and the parent account, two identical LE folders are created. One folder will be maintained by the EKMS Manager and the other maintained by the LE command. Each folder contains tabs for forms, letters and correspondence. The LE folder shall be made available to the EKMS Manager or an EKMS Inspector upon request.

3.3 Access List. Enter the names of all persons having access to material on a formal access list signed by the current CO. The CO may grant access to cleared and uncleared visitors as required. Uncleared visitors must be continuously escorted by a properly cleared person whose name is on the access list.

Note: When uncleared repair personnel who are admitted to perform maintenance on commercially contracted information processing equipment, connected to circuits, protected by cryptographic equipment, must be escorted by a CRYPTO-repair person or other technically qualified person.

3.4 Visitor Register. Record all visits in the visitor register and retain the register for at least 1 year after the date of the last entry. The visitor register, at a minimum, will contain the following:

   a. Date/time of arrival and departure.
   b. Printed name and signature of visitor.
   c. Purpose of visit.
   d. Signature of authorized individual admitting the visitor(s).

3.5 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., birth dates, social security numbers and phone numbers).

a. Requirements for Changing a Combination

(1) When the lock is initially placed in use, change the manufacturer preset combination.

(2) When any person having knowledge of the combination no longer requires access (e.g., loss of clearance, transfer), unless other sufficient controls exist to prevent access to the lock.

(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) When any repair work performed was on the combination lock.

(5) At least once every 2 years or sooner as dictated by the above events.

b. 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 to personnel authorized to change safe or COMSEC facility combinations. Only cleared individuals, who have been formally authorized access to COMSEC keying material by the CO, shall change combinations.

c. Classification of Combinations. Lock combinations providing access to COMSEC material shall be classified SECRET and protected as such.

d. Sealing/Wrapping Combinations

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

(2) Laminate each envelope in plastic (similar to an identification card).
(3) The name(s) and address(es) of the individual(s) authorized access to the combinations must be recorded on the front of the envelope.

(4) Store the SF-700 in a General Services Administration (GSA) approved security container. An approved GSA security container will have a red or black label affixed to the top drawer. The label will read "General Services Administration Approved Security Container" listing as the manufacturer Mosler or Mas Hamilton.

Note: (1) SF-700: Part (1) of a classified container information form (Standard Form 700 (8-85) for each lock combination must be placed on the inside of each COMSEC storage container. Part 1 is not classified. A change to Department of Defense (DoD) policy considers personal addresses and telephone numbers to be Personally identifiable information and requires Part 1 be sealed in a non-opaque envelope prior to posting inside the container or door, as applicable. Both Parts 2 and 2A will be classified based on the classification of the highest content in the container and must reflect the following derivative and downgrading instructions:

"Derived from: 32 CFR 2001.80(d)(3)"
"Declassify: Upon Change of Combination".

e. Personal Retention of Combination. It is specifically prohibited for an individual to record, 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.

f. If the secure enclave/COMSEC facility or COMSEC storage container is found opened without cleared and authorized personnel present perform the following:

   (1) Post a guard.

   (2) Notify the Command Duty Officer.

   (3) The person responsible for the container must conduct an inventory.

   (4) Notify COMNAVRESFORCOM EKMS Manager and Information Security Manager and the CNRF ISIC.

Enclosure (1)
3.6 Communications Security Training. All personnel designated as LE Custodian must complete the applicable portions of the latest version of NAVEDTRA 43462 (EKMS PQS). The PQS is intended to supplement, through hands-on training at the unit level.

COMNAVRESFORCOM EKMS personnel will conduct monthly LE training and additional training as required. All LE Custodians and LE Alternate Custodians are required to attend all training session held by EKMS account Personnel.

3.7 Commanding Officer Spot Checks. LE COs are required to conduct one spot check per quarter. CO spot checks are conducted per the EKMS for Commanding Officers Handbook. The CO may delegate no more than two spot checks to the Executive Officer. Upon completion of CO spot checks, the LE’s are required to electronically forward a signed, completed spot check to the parent account.

3.8 Destruction. Effective and superseded keying material is extremely sensitive and increases the risk of compromising all encrypted information. For this reason, keying material must be destroyed as soon as possible after it has been superseded or has otherwise served its intended purpose. The custodian will be contacted by the EKMS Manager when destruction of COMSEC keying material is to be conducted.

   a. COMSEC material that is authorized for destruction must be destroyed by the LE Custodian and LE Alternate Custodian. Authorization for destruction by LE’s shall come from the parent command EKMS account Manager.

   b. When electronic COMSEC keying material is intentionally or unintentionally destroyed report and forward destruction via an SF-153 destruction report to the parent EKMS account manager. See figure 3.1.

Enclosure (1)
**Figure 3.1 SF-153 Destruction Report**
3.9 Emergency Action Plan. LE commands shall maintain a current, written Emergency Action Plan (EAP) for safeguarding COMSEC material (e.g., KG-175D (TACLANE), secure modems, Data Transfer Devices (DTDs), electronic keying material, KSV-21 cards, KOV-26 and Crypto Ignition Keys (CIKs) in the event of an emergency. The EAP must be reviewed at least annually.

   a. Emergency planning must consider natural disasters (e.g., fire, flood, tornado and earthquake) likely to occur in your region of the country as well as hostile actions (terrorist attack, rioting or civil uprising).

   b. Emergency planning for hostile actions must concentrate on procedures to safely evacuate or securely destroy the COMSEC material, to include providing for the proper type and a sufficient number of destruction devices to execute emergency destruction.

   c. Emergency planning for natural disasters should be directed toward maintaining security control over the material until the situation stabilizes, taking into account the possible loss of normal physical security protection that might occur during and after a natural disaster.

   d. All authorized personnel at the facility must be aware of the existence of the EAP.

   e. Emergency Planning for disasters must provide for:

      (1) Fire reporting and initial fire fighting by assigned personnel.

      (2) Assigning of on-the-scene responsibility for ensuring protection of COMSEC material held.

      (3) Securing or removing classified COMSEC material and evacuating the area(s).

      (4) Protecting COMSEC material when admitting outside emergency personnel into the secure area(s) is necessary.

      (5) Assessing and reporting probable exposure of classified COMSEC material to unauthorized persons during the emergency.

      (6) Conducting post-emergency inventory of classified COMSEC and Controlled Cryptographic Item (CCI) material and
reporting any losses or unauthorized exposure to the EKMS Manager authorities.

f. Conduct annual EAP training exercises to ensure that personnel are familiar with assigned duties.

g. Review EAP annually and update as necessary or whenever changes in the local environment dictate an update to the plan.

h. Most LE commands are issued KG-175D (TACLANE) and associated CIKs, STE terminal and associated KSV-21 card. On occasion, a secure modem and DTD may be issued. During an emergency condition consider zeroizing all equipment and placing into a GSA approved space in your secure enclave.
4.1 Secure Terminal Equipment. The STE is the new generation of secure voice and data equipment replacing the STU-III telephone. The security core is the KSV-21 cryptographic card which provides all security services. The KSV-21 card is a high-grade security token with built-in U.S. Government-owned encryption algorithms and public key exchange protocols.

a. Responsibilities and Duties

(1) The STE and KSV-21 card will be issued to the LE command and signed for by the LE Custodian. The LE CO is solely responsible for safeguarding the card and cannot transfer the card to another individual without the authorization of the parent EKMS account.

(2) The LE Custodian may allow or permit others to use issued card as long as the person is cleared to the security level of the keys programmed on the card.

(3) The LE Custodian must protect the KSV-21 card by storing it in a manner that will minimize the possibility of loss, unauthorized use, substitution, tampering or breakage.

b. STE Accountability, Classification and Handling

(1) The STE is UNCLASSIFIED equipment and does not require accountability within the CMCS, meaning it is not CCI. The STE is a high dollar value, sensitive, pilferable item; therefore, local command property accounting and security controls must be strictly adhered to. The STE must be protected in a manner sufficient to prevent loss and tampering. A STE with a KSV-21 card inserted may not be left unattended to prevent possible unauthorized use. However, the STE may be left unattended when the KSV-21 cryptographic card is not inserted. In the event the STE telephone becomes inoperable immediately contact the parent account to verify the status of manufacturer’s warranty. The parent account will advise on disposition.

(2) KSV-21 accountability. The KSV-21 card contains cryptography and is accounted for within the CMCS until the card is physically destroyed. Use the Central Index Key Data Log to locally account for the KSV-21 card. The unique serial number is be used for accountability. The KSV-21 card is classified as SECRET. When the KSV-21 card is inserted into the telephone,
the STE becomes classified to the SECRET level. When the KSV-21 card is removed the STE becomes UNCLASSIFIED.

(3) All operational keys have a one-year crypto period. At the end of the crypto period, the user must call the EKMS Central Facility for new operational keys. Rekey calls may be placed at any time prior to the expiration date. Once the rekey calls are complete, the user must verify that the dates have changed and have been extended for another year.
5.1 Forms. To facilitate proper administration and management of COMSEC material various forms are utilized. Each form has a specific purpose and their use is mandatory.

a. SF-153 COMSEC Material Report. Form SF-153 COMSEC Material Report (Figure 5.1) is a multi-purpose form used to record COMSEC material transactions (e.g., transfer, receipts, inventories). Every transaction of COMSEC material will use the SF-153 form. The following are signature requirements for the SF-153 COMSEC Material Report:

(1) "Hand Receipt." COMSEC material issued to LE.
Minimum signature, LE Custodian, witness.

(2) "Inventory." Forward to LE to conduct physical inventory of COMSEC material.
Minimum signature, LE Custodian, witness and CO.
Return completed inventory within 96 hours.

(3) "Destruction." Destruction of COMSEC material either physical or electronic.
Minimum signature, LE Custodian, witness and CO.

(4) "Other." Used by LE to return COMSEC material to the EKMS Manager. LE signature not required. When received by the parent account, the EKMS Manager/Alternate Manager will generate and sign a SF-153 from the parent EKMS account and return copy to LE for tracking.
Figure 5.1 SF-153 COMSEC Material Report

Enclosure (1)
b. **SF-700 Security Container Information.** Form SF-700 Security Container Information (figure 5.2) is used to maintain a record for each security container, vault or secure room door showing the location of each person by name, home address and home telephone number, having knowledge of the combinations and who is to be contacted in the event the security container, vault or secure room is found open and unattended. Update SF-700s as required due to staff turnover.

(1) Place part 1 of the completed SF-700 on an interior location in security containers, vault or secure room doors.

(2) Parts 2 and 2A will be classified based on the classification of the highest content in the container and must reflect the following derivative and downgrading instruction:

"Derived from: 32 CFR 2001.80(d)(3)"
"Declassify: Upon Change of Combination”.

(3) Store parts 2 and 2A in a security container other than the one to which it applies. If necessary, continue the listing of persons having knowledge of the combination on an attachment to part 2.

![Figure 5.2 SF-700 Security Container Information](image)

---

c. **SF-701 Activity Security Check List.** Form SF-701 Activity Security Check List (Figure 5.3) is used to conduct end of the day security checks to ensure all areas which process classified information are properly secured. The SF-701 may be
destroyed 30 days after the last entry, unless used to support an ongoing investigation.

| ITEM | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 1. Security containers have been sealed and checked. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2. Desks, shelves and other surfaces are free of classified material. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3. Windows and doors have been locked (where applicable). | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4. Transfer boxes and AOP devices (i.e., data, tapes) containing classified material are free of classified material. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5. Security devices and equipment have been activated (where applicable). | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Figure 5.3 SF-701 Activity Security Check List**

Enclosure (1)
d. SF-702 Security Container Check Sheet. Form SF-702 "Security Container Check Sheet" (Figure 5.4) will be annotated whenever a security container, vault or secure room is opened or closed and at the end of each work day to ensure the container is properly secured. The SF-702 will be posted in a conspicuous area outside of the security container, vault or secure room. Users will ensure the SF-702 is posted the first duty day of each month and maintained for 30 days. The SF 702 must have a daily entry, even if not opened and must have an end of day entry.
Figure 5.4 SF-702 Security Container Check Sheet

Enclosure (1)
e. Optional Form 89 Maintenance Record for Security Containers and Vaults. Optional Form 89 is used to record maintenance on the lock (lock replacement). The form is to be placed on the inside of a security container drawer or vault door. See Figure 5.5.

![Maintenance Record for Security Containers/Vault Doors](image-url)

**Figure 5.5 Optional Form 89 Maintenance Record for Security Containers/Vault Doors**

Enclosure (1)
f. Crypto Ignition Key (CIK) Data Log. The CIK Data Log (Figure 5.6) is used to track individual key storage devices (KSV-21), more commonly referred to as "STE Card." In most cases, you will be issued one KSV-21 Card. Use of this form is mandatory. You may obtain an electronic copy from the parent EKMS account.

Enclosure (1)
**COMNAVRESFORCOM LE**

**CRYPTO IGNITION KEY DATA LOG**

Command:
EKMS Account: 177015

<table>
<thead>
<tr>
<th>ID of card associated with STE</th>
<th>STE SER NO. in which key is loaded</th>
<th>Where Terminal is installed (Bldg/Rm)</th>
<th>Date card created or date terminal keyed</th>
<th>Card serial number</th>
<th>N - Master U - User</th>
<th>Card Sequence (1 OF ?)</th>
<th>ID of Key User</th>
<th>Phone number of card user</th>
<th>Date card deleted or zeroized</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**STE Terminal** KSV-21

Figure 5.6 Crypto Ignition Key Data Log

Enclosure (1)
6.1 Request for Communications Security Material. In order to request COMSEC material, LE Custodian must contact the parent account with their request via digitally signed E-MAIL (preferred), or a phone call.

6.2 Shipping Communications Security Material. Whenever COMSEC material is shipped between the parent account and LE, an SF-153 "Hand Receipt" or "Other" (return to EKMS Manager) report will be placed in each package of COMSEC material. See Figure 6.1 and 6.2.

   a. Method of shipment. FedEx courier is the method of shipment for COMSEC material between the parent account and LEs. This method affords electronic point-to-point accountability.

      (1) The transferring command (parent account or LE) must notify the intended recipient, within 24 hours, with the tracking number and a list of COMSEC material shipped via digitally signed email.

      (2) If a shipment is not received within five working days of the expected delivery, contact the parent account immediately.

   b. Wrapping requirements. All COMEC keying material must be double-wrapped, using a non-transparent wrapper and securely sealed.

      (1) Inner wrapper. When shipping CCI separately, the classification is unclassified; therefore you will not need a marking on the inner wrapper. Inner wrapping must contain the following information.

         (a) “To” and “From” addressees.

         (b) EKMS account number of both the shipping and receiving command.

         (c) “CRYPTO.”

         (d) Controlled package number (FedEx tracking number).

         (e) “TO BE OPENED ONLY BY EKMS MANAGER.”

Enclosure (1)
Note: Please be aware the CCI each LE maintains is only classified when initialized (when the KSV-21 card is placed in the phone or when the CIK is inserted in the Taclane KG-175D).

(2) **Outer wrapper.** The outer wrapper must be marked with the following information:

(a) "To" and "From" addresses.

(b) Any applicable notations to aid delivery (i.e., Attention EKMS Manager.

Note: The outer wrapper must never reveal whether the package contains classified information or keying material. The contents of the package are not to be disclosed in any manner on the outer wrapper.

c. **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 corresponding keying material cannot be physically separated.

(2) Package primary and associated keying material (e.g., KG-175D, associated master and user keys) separately within one shipment.

6.3 **Receiving and Opening Communications Security Material Shipments**

a. Inspect inner and outer wrapper for signs of tampering.

b. Open shipment.

c. Inventory the contents against the SF-153.

d. Receipt for material and return signed report to the parent account fax or digitally scanned and emailed.

e. File copy of report in LE Folder.

f. Properly store the material.

Enclosure (1)
### Figure 6.1 SF-153 Hand Receipt

This form is FOR OFFICIAL USE ONLY unless otherwise stamped.

<table>
<thead>
<tr>
<th>SHORT TITLE/DESIGNATOR - EDITION</th>
<th>QUANTITY</th>
<th>ACCOUNTING NUMBERS</th>
<th>BEGINNING</th>
<th>ENDING</th>
<th>A/LD</th>
<th>REMARKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>FNBB 21</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KG 175</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Total Quantity=2**

**Number of Line Items=2**

Recipient will fill in box 14 "RECEIVED", 15a,b,c,d

**Figure 6.1 SF-153 Hand Receipt**

Enclosure (1)
Figure 6.2 SF-153 Other (Return to EKMS Manager)
7.1 Communications Security Inventories

a. The parent EKMS account must conduct a Fixed Cycle (FC) COMSEC material inventory in January and July of each year. An additional inventory is required for change of command and change of manager. The parent account will generate a COMSEC inventory for each LE and forward via e-mail or fax. The inventory must be completed, signed and returned to the parent account within 5 working days of receipt. See figure 7.1 for an example of an SF-153 Inventory Report.

b. The LE will also receive a LE Questionnaire (figure 7.2) with their inventory report. The data is used to update the LE Tracking Tool data base.
### Figure 7.1 SF-153 COMSEC Inventory Report

<table>
<thead>
<tr>
<th>Item</th>
<th>Quantity</th>
<th>Accounting Numbers</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) FNBB21</td>
<td>1</td>
<td>SN: 21001234</td>
<td></td>
</tr>
<tr>
<td>2) KG 175</td>
<td>1</td>
<td>SN: 12345</td>
<td></td>
</tr>
</tbody>
</table>

**Total Quantity:** 2  
**Number of Line Items:** 2  
**Reason For Inventory:** Semi Annual  
**Latest Transaction ID:** 177015 20070831 01234

**Blk 15 a-d:** Outgoing CO  
**Blk 16 a-d:** Incoming CO  
**Blk 17:** Outgoing CO Print & Sign.

**LE check “INVENTORY” & “WITNESS” box**
Figure 7.2 LE Questionnaire
Chapter 8

8.1 Communications Security Incidents. In the event of a COMSEC incident, the LE Command will immediately report the incident (Figure 8.1) to the EKMS Manager. The information provided must be of sufficient detail to enable the account EKMS Manager to assume responsibility for reporting the incident via naval message. COMSEC incidents are evaluated as:

a. Cryptographic incident reports.

b. Personnel incident report.

c. Physical incident report.

---

Command Letter Head

SSIC Code/Serial Date
From: Commanding Officer, "LE Command"  
To: EKMS Manager, Commander, Navy Reserve Forces Command  
Subj: COMSEC INCIDENT REPORT  
Ref: (a) EKMS 18  
(D) CNRFC INST 2280  
Encl (1) Title or material enclosed with letter as applicable
1. Local Element Command:
2. COMSEC Material Type:
3. Personnel involved:
4. Circumstances:
5. Estimate of compromise:
6. Details of incident: Refer to EKMS 18 para 970 d(6)
7. Investigation: State whether an investigation has been initiated (e.g., local command inquiry, NCIS, JAG).
8. Command point of contact:

I.B. ZEUS  
CDR. USN

---

Figure 8.1 LE COMSEC Incident Report

Enclosure (1)
Chapter 9

9.1 Practices Dangerous to Security (PDS). PDS are reportable to the parent account and are practices, which have the potential to jeopardize the security of COMSEC material, if allowed to perpetuate. See Figure 9.1. The following is a list of non-reportable PDS:

a. Improperly completed accounting reports (i.e., unauthorized signatures, missing signatures or required accounting information).

b. COMSEC material not listed on LE inventory when documentation exists at the parent account to indicate that the material was issued to the LE.

c. Receipt of a package with a damaged outer wrapper, but an intact inner wrapper.

d. 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.

e. Not completing and returning the FC inventory within 4 days of receipt except where a waiver has been granted.

f. No change of command/LE Custodian inventory conducted.
From: Commanding Officer, "Local Element Command"
To: Electronic Key Management System Manager, Commander, Navy Reserve Forces Command

Subj: PRACTICE DANGEROUS TO SECURITY

Ref: (a) EKMS 1B
     (b) COMNAVRESFORCOMINST 2280.1B

1. Local Element Command:

2. Personnel involved:

3. Details of PDS:

4. Corrective Action to prevent re-occurrence:

I. B. ZEUS
CDR, USN

Figure 9.1 LE PDS Letter
Chapter 10

10.1 Navy and Marine Corps Intranet Secret Internet Protocol Router Network. COMNAVRESFORCOM will provide cryptographic items and keying material to Information Security personnel. The following procedures apply:

a. MOU between parent account and Local Element.

b. Parent account issue LE Custodian cryptographic items and keying material on local custody.

c. NMCI ISF personnel must be listed on the NAVOPSPTCEN Security Access List to space(s) in which they require access to perform required duties.
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.

Accountable Item Summary - A list of all COMSEC material held at your command.

Account Clerk - An individual assigned to assist EKMS account personnel in the execution of certain administrative duties associated with the management of an EKMS account.

Accountability Legend Code - Accountability Legend (AL) codes determine how COMSEC material is accounted for within the CMSC. Five AL codes are used to identify the minimum accounting controls required for COMSEC Material.

AL 1: COMSEC material is continuously accountable to the Central Office of Record by serial number from production to destruction (i.e., KG-175D, STE, KOV-26, KSV-21, etc.).

AL 2: COMSEC material is continuously accountable to Central Office of Record by quantity from production to destruction.

AL 4: After initial receipt to the Central Office of Record, COMSEC material is locally accountable by quantity and handled/safeguarded based on its classification (i.e., STE and KG-175D CIKs).

AL 5: COMSEC material that is electronically generated and continuously accountable to the Central Office of Record from production to destruction.

AL 6: COMSEC material that is electronically generated and locally accountable to the COMNAVRESFORCOM EKMS account.
Commanding Officer - Individual ultimately responsible for the proper administration of their COMSEC material holdings and compliance with established EKMS policy and procedures.

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.

COMSEC Facility - Space employed primarily for the purpose of generating, storing, repairing or using COMSEC material.

COMSEC Incident - Any uninvestigated or unevaluated occurrence that has the potential to jeopardize the security of COMSEC material or the 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.

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.

Crypto-Equipment - Equipment that embodies a cryptographic logic (i.e., KG-175D, KIV-7, KOV-26, KSV-21).

Controlled Cryptographic Item - COMSEC material defined as a secure telecommunications or information handling equipment or associated cryptographic component, which is unclassified but controlled.

Crypto-Ignition Key - Device or electronic key used to enable secure operations of crypto-equipment (KSV-21, KOV-26, KG-175D Special Security Officer and User Key).

Cryptoperiod - Time span during which each key setting remains in effect.

Cryptosystem - Associated COMSEC items interacting to provide a single means of encryption or decryption.

Data Transfer Device - A fill device used to store and distribute electronic key.

Enclosure (1)
EKMS Manager - An individual designated by his/her Commanding Officer to be responsible for all actions associated with receipt, handling, issue, safeguarding, accounting and disposition of COMSEC material/equipment assigned to a command’s EKMS numbered account.

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.

External LE - Individual(s) requiring COMSEC support and whose Commanding Officer is other than the account EKMS Manager. These are NAVOPTSPTCEN(s), Squadron(s) and Region(s), etc.

Fill Device - Any one of a family of devices developed to read in transfer or store key (i.e. STE, Simple Key Loader and DTD).

Hand Receipt - A document used to record custody of COMSEC material given to or received from manager personnel or a CMS user.

Highest Classification Indicator - Highest Classification Indicator is used to determine the highest classification of COMSEC material that an account may hold.

Immediate Superior in Command - Command responsible for the administrative oversight of all EKMS matters for their subordinate commands. COMNAVRESFOR is your Immediate Superior in Command.

Insecure Practices - Occurrences, which, although not reportable outside the violating command, have the potential to jeopardize the security of COMSEC material if allowed to perpetuate.

Internal LE - Individual(s) and EKMS account are assigned to the same command (i.e., COMNAVRESFORCOM (N3), (N5), etc.).

Keying Material - A type of COMSEC item in physical or electronic 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.
Local COMSEC Management Software - Software which resides on the local management device and performs functions such as accounting, auditing, distribution ordering, production, system administration, operator interface services and platform dependent services. Local COMSEC Management Software is used by the COMNAVRESFORCOM EKMS Manager.

LE Custodian - Individual(s) appointed, in writing, by the CO responsible for administering and managing COMSEC material issued to their command.

Local Management Device - Computer which provides automated services for management of key and other COMSEC material and an interface by which additional functionality may be incorporated to enhance its local capabilities. The Local Management Device is used by the COMNAVRESFORCOM EKMS Manager.

SF-153 - Multi-purpose form used to record COMSEC material transaction (receipts, transfers, destructions, inventories).

Staff CMS Responsibility Officer (SCMSRO) - An individual (0-4 or above), designated by a flag or general officer in command status, responsible for the proper administration of routine EKMS account matters.

STE User - An individual or group of individuals who use STE terminals and KSV-21 to make secure calls, regardless of whether or not they have personally signed for the material on local custody.

Supersession - Scheduled or unscheduled replacement of COMSEC material with a different edition.

Transaction Number - A number used to maintain continuity of COMSEC material transactions.

Zeroize - To remove or eliminate the key from a crypto-equipment or fill device.
Annex B

Retention Periods

1. 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. **SF-153 Local Custody Documents.** Retain for 90 days after supersession.

   b. **Memorandum of Understanding.** Retain for 1 year after COMSEC support has been terminated.

   c. **Appointment Letters.** Retain for 2 years from the date an individual has been relieved of his/her duties.

   d. **Local Holder CBT Certificate.** Retain for 2 years from the date an individual has been relieved of his/her duties.

   e. **Inventory Report.** Retain inventory report for 2 years.

   f. **Visitor Register.** Retain for 1 year from the date the register has been completed.

   g. **Destruction Reports.** Retain for 2 years.

   h. **Correspondence.** Retain general correspondence and all other messages relating to only LE holdings for 2 years.

   i. **Directives and Instructions.** Retain required items related to LE holdings until cancelled or superseded.

   j. **Other.** (i.e. mail, FedEx TN, mail) retain for 1 year.

   k. **COMSEC Facility Inspection.** All required inspections must be documented and records maintained on file at the facility and the cognizant security officer for 3 years.

   l. **CIK Data Log.** Retain for 90 days following the date of the last recorded log entry.

   m. **Spot Checks.** CO/Executive Officer spot checks are inspectable items and should be retained until the next parent account EKMS inspection is conducted.

Enclosure (1)