DEPARTMENT OF THE NAVY
COMMANDER NAVY RESERVE FORCES COMMAND
1915 FORRESTAL DRIVE
NORFOLK VA 23551-4615

COMNAVRESFORCOMINST 2280.1G
N6
5 Mar 2025

COMNAVRESFORCOM INSTRUCTION 2280.1G

From: Commander, Navy Reserve Forces Command

Subj: KEY MANAGEMENT INFRASTRUCTURE OPERATING ACCOUNT ADMINISTRATION AND MANAGEMENT PROCEDURES

Ref: (a) CMS-1A AMD-1
(b) CMS-3A AMD-1
(c) SECNAVINST 5510.36B
(d) SECNAV1NST 5510.30C
(e) KMI 5110 version 1

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

1. Purpose. Provide policy and procedures for administration, management and handling of Communication Security (COMSEC) material within the Navy Reserve Force per references (a) through (e).

2. Cancellation. COMNAVRESFORCOMINST 2280.1F.

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. It provides 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 and could result in prosecution of the parties concerned under the espionage laws, Title 18. U.S.C. §793, 794 and 798.

a. LE commanding officers are not authorized to appoint or assign contractor personnel as LE custodians or as a COMSEC user.

b. Enclosure (1) is COMNAVRESFORCOM LE COMSEC administration and management procedures which contain applicable portions of references (a) through (e). It should be used by all LEs and COMSEC users who receive, store and use COMSEC material issued from COMNAVRESFORCOM KMI operating account 177015. Commands not supported by COMNAVRESFORCOM KMI operating account 1 77015 should adhere to the policy and procedures of their parent account.

5. Scope. The guidance herein supplements, but in no way alters or amends the provisions of U.S. Navy Regulations and references (a) through (e).

6. Action. Navy Reserve Region Readiness and Mobilization Commands (REDCOMs) Commanders, LE commanding officers, Navy and Marine Corps Internet (NMCI) information managers, LE custodians and COMSEC users are directed to enforce and adhere to the provisions set herein.

7. Comments. Submit comments, recommendations, and suggestions for changes to COMNAVRESFORCOM KMI operating account manager.

8. Records Management. Records created as a result of this instruction, regardless of media and format, must be managed per Secretary of the Navy Manual 5210.1 of September 2019.

9. Review and Effective Date. Per OPNAVINST 5215.17A, COMNAVRESFORCOM N01A will review this instruction annually around the anniversary of its issuance date to ensure applicability, currency, and consistency with Federal, Department of Defense, Secretary of the Navy, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will be in effect for 10 years, unless revised or cancelled in the interim, and will be reissued by the 10-year anniversary date if it is still required, unless it meets one of the exceptions in OPNAVINST 5215.17A, paragraph 9. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the need for cancellation is known following the guidance in OPNAV Manual 5215.1 of May 2016.

M. J. STEFFEN

Releasability and distribution:
This instruction is cleared for public release and is available electronically only via COMNAVRESFOR Web site, http://www.public.navy.mil/nrh/Pages/instmctions.aspx

COMMANDER, NAVY RESERVE FORCES COMMAND

LOCAL ELEMENT COMMUNICATIONS SECURITY ADMINISTRATION AND MANAGEMENT PROCEDURES

Foreword

The primary purpose of this publication is to provide detailed guidance to Local Element (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 ensures to COMSEC material and facilities IAW CMS-1A AMD-1.

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, CMS-1A AMD-1, SECNAVINST 5510.36A and SECNAVINST 5510.30B.

Table of Contents

Chapter 1

1.1. Key Management Infrastructure (KMI) Account Information.

KMI Operating Account Number: 177015
Highest Classification Indicator: Secret

Mailing Address:
COMNAVRESFORCOM
ATTN: KMI Manager
1915 Forrestal Drive
Bldg. NH-32
Norfolk, VA 23551-4165

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

Contact Information:
KOA Manager: (948)223-6277
Alternate KOA Manager: (948)223-6277
COMSEC Account Clerk: (948)223-6277
Email address: cnrfc_kmi_managers@us.navy.mil

1.2. 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 Secret Internet Protocol Network (SIPRNet), and KG-175D (TACLANE).

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. 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) and KMI Operating Accounts (KOAs), is known collectively as the COMSEC Material Control System (CMCS).

b. 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. Commander, Navy Reserve Forces Command (COMNAVRESFORCOM) is assigned COMSEC account number 177015.

1.3. 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 a COMSEC Management Team to administer and manage his/her COMSEC program. Applying structured processes and procedures, the COMSEC Management Team tracks each individual piece of COMSEC material from initial receipt to issuance and destruction.

Figure 1.1 represents the COMSEC chain of command.

a. Immediate Superior in Command (ISIC). Commander, Navy Reserve Force (COMNAVRESFOR) 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 SCMSRO reports directly to the Commander, and the KOA Manager reports directly to the SCMSRO on all matters relating to COMSEC material management.

c. Commanding Officer (CO). The CO is responsible for properly administering COMSEC holdings, ensuring compliance with this instruction and established policies and procedures.

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

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

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

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 Navy Reserve Region Readiness and Mobilization Command (REDCOM) while supporting tasking from COMNAVRESFORCOM; however, they are accountable to the Commander, reporting directly to the KOA Manager for matters relating to COMSEC material administration and management.

Chapter 2

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. A Memorandum of Understanding (MOU) must be exchanged between COMNAVRESFORCOM and the command requesting COMSEC support. The MOU establishes the terms and conditions of support and requires the signature of the requesting command's CO and SCMSRO. This shall be renewed for every change of command turnover.

b. Facility Approval. As a condition outlined in the MOU, the requesting command must provide to the KOA 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 CMS-1A AMD-1 and CMS-3A AMD-1.

c. LE Custodian Appointment. LE Custodians must be designated in writing by the LE CO. Each LE must appoint, in writing, two LE Custodians 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 KMI Personnel Qualification Standards (PQS) Naval Education and Training (NAVEDTRA) 43462-2A.

(5) Complete COMSEC User Acknowledgement Form.

(6) Hold an LE appointment letter.

Note 1: The COMSEC account holder will forward all required forms, templates and briefs. Retain each form and letter in the LE folder on SharePoint drop box, LE may keep a local copy on hand.

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

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

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

d. REDCOM. REDCOMs do not manage COMSEC material, REDCOMs are administratively responsible for managing the accountability of COMSEC material. The REDCOM monitors, tracks and reports on COMSEC compliance and deliverables to the KOA Manager. The REDCOM will consolidate reports and gather the status of assigned tasking for further submission to the KOA Manager. REDCOMs do not provide direction on the administration and management of LE COMSEC holdings.

Chapter 3

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. Deviation from these principals significantly increases 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 the LE and the parent account, two identical LE folders are created. One folder will be maintained by the KOA Manager and the other maintained by the LE command. The LE folder shall be made available to the KOA Manager or a COMSEC 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 not-cleared visitors as required. Visitors who are not cleared, must be continuously escorted by a properly cleared person whose name is on the access list.

Note: Technicians who are not cleared, but 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 one 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 the 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, 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 two 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 an 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. Department of Defense (DoD) policy considers personal addresses and telephone numbers to be Personally identifiable information (PII) 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 unsecured 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 KOA Manager/Alternates.

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

3.6. Communications Security Training. All personnel designated as LE Custodians must complete the applicable portions of the latest version of NAVEDTRA 43462 (KMI PQS). The PQS is intended to supplement, through hands-on training at the unit level. COMNAVRESFORCOM COMSEC personnel will provide monthly LE training and additional training as required. All LE Custodians are required to receive all training sessions.

3.7. Commanding Officer Spot Checks. LE COs are required to conduct one spot check per quarter. CO spot checks are conducted per the COMSEC Management in the CMS-3. The CO may delegate no more than two spot checks to the Executive Officer. Upon completion of CO spot checks, the LEs are required to electronically forward a signed, completed spot check to the parent account via SharePoint.

3.8. Emergency Action Plan (EAP) / Emergency Destruction Plan (EDP). All commands are required to have an EAP/EDP local policy on file as well as annual training completed IAW SECNAVINST 5500.35.

Chapter 4

4.1. 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. Standard Form 153 (SF-153) COMSEC Material Report. Form SF-153 COMSEC Material Report (Figure 4.1) is a multi-purpose form used to record COMSEC material transactions (e.g., transfer, receipts, and 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 (Block 15), witness (Block 16).

(2) "Inventory." Forward to LE to conduct physical inventory of COMSEC material. Minimum signature: LE Custodian (Block 15), witness (Block 16) and CO (Block 17).

(3) "Destruction." Destruction of COMSEC material either physical or electronic. Minimum signature: LE Custodian (Block 15), witness (Block 16) and CO (Block 17).

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

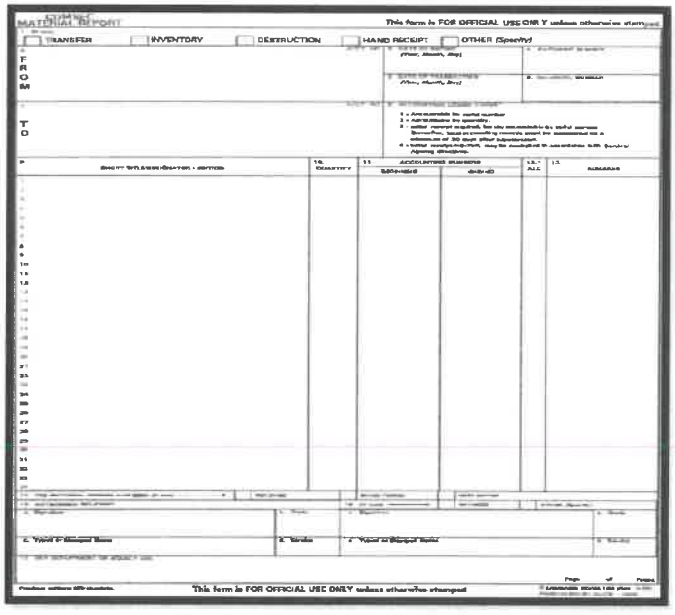


Figure 4.1 SF-153 COMSEC Material Report

b. Standard Form 700 (SF-700) Security Container Information. Form SF-700 Security Container Information (figure 4.2) 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 other than the one to which it applies. The listing of persons having knowledge attachment to part (2).

Figure 4.2 SF-700 Security Container Information

c. Standard Form 701 (SF-701) Activity Security Check List. Form SF-701 Activity Security Check List (Figure 4.3) 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.

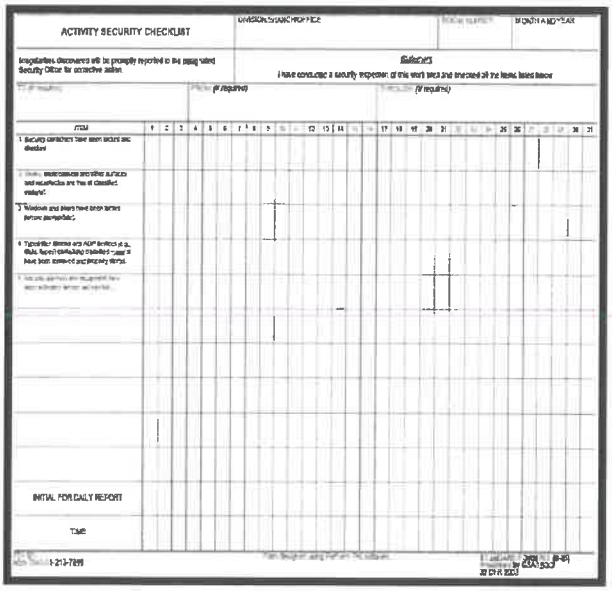


Figure 4.3 SF-701 Activity Security Check List

d. Standard Form 702 (SF-702) Security Container Check Sheet. Form SF-702 "Security Container Check Sheet" (Figure 4.4) 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 a new SF-702 is posted the first duty day of each month. The previous month's forms are to be retained for 30 days after final entry. The SF 702 must have a daily entry for working days, even if security container is not opened, and must also have an end of working day entry.

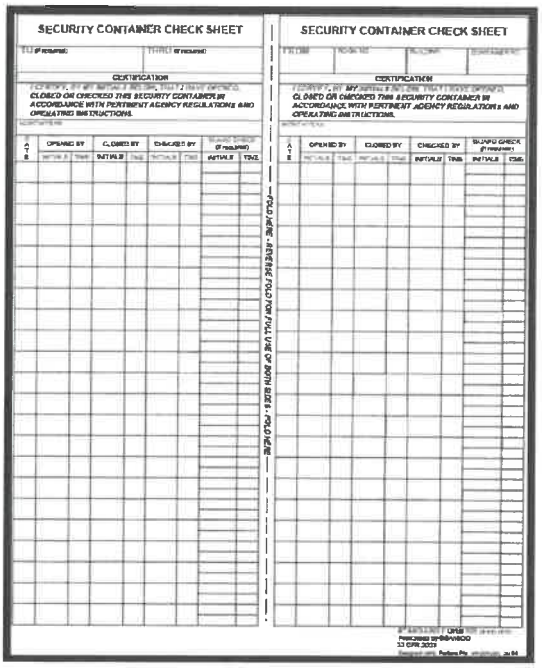


Figure 4.4 SF-702 Security Container Check Sheet

e. Optional Form 89 (OF-89) Maintenance Record for Security Containers and Vaults. OF-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. The OF-89 is to be retained for the life of the container. See Figure 4.5.

Figure 4.5 Optional Form 89 Maintenance Record for Security Containers/Vault Doors

Chapter 5

5.1. Request for Communications Security Material. In order to request COMSEC material, LE Custodians must contact the parent COMSEC account with their request via digitally signed email.

5.2. Shipping Communications Security Material. Whenever COMSEC material is shipped between the parent account and LE, an SF-153 "Hand Receipt" report will be placed in each package of COMSEC material. See Figure 5.1.

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 COMSEC 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) KMI account number of both the shipping and receiving command.

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

Note: Please be aware the CCI each LE maintains is only classified when initialized (when the CIK is inserted in the KG-175O TACLANE).

(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: KOA Manager).

Note: 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-1750, associated master and user keys) separately.

5.3. 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.

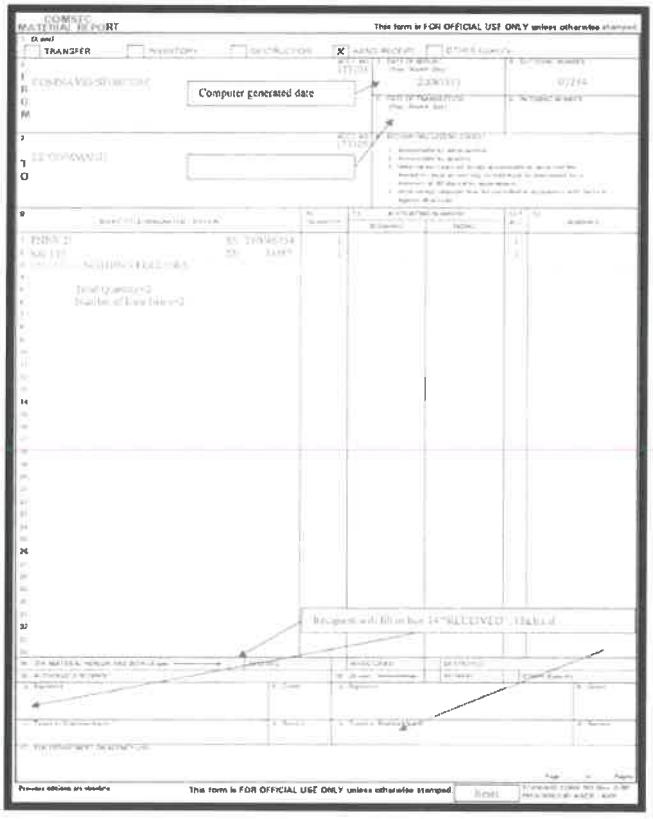


Figure 5.1 SF-153 Hand Receipt

Chapter 6

6.1. Communications Security Inventories (SF-153)

a. The parent COMSEC account (CNRFC KMI) must conduct a Fixed-Cycle (FC) COMSEC material inventory -in February and August of each year. LE Commands will conduct FC inventories in January and July. Additional inventories are required for changes of command and changes of manager. The parent account will generate a COMSEC inventory for each LE and will forward. See figure 6.1 for an example of an SF-153 Inventory Report.

b. The LE will submit an updated LE Questionnaire with their fixed-cycle inventory report or when applicable.

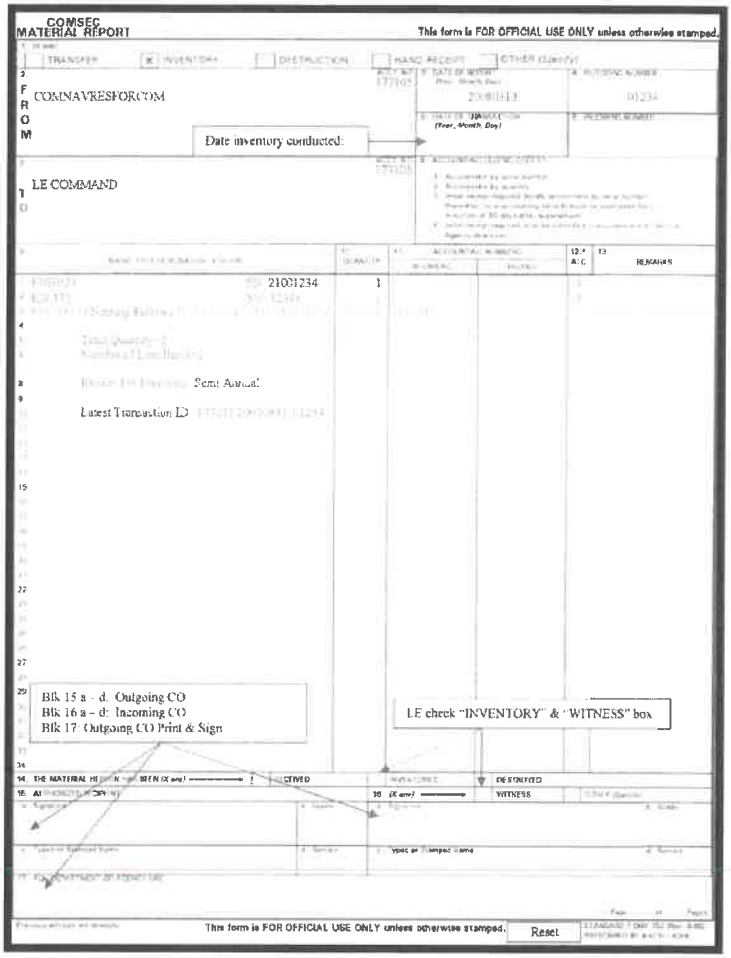


Figure 6.1 SF-153 COMSEC Inventory Report

Chapter 7

7.1. Communications Security (COMSEC) Incidents. In the event of a COMSEC incident, the LE Command will immediately report the incident (Figure 7.1) to the KOA Manager (CNRFC KMI Team). The information provided must be of sufficient detail to enable the KOA Manager to assume responsibility for reporting the incident via Naval Message. COMSEC incidents are evaluated as:

a. COMSEC incidents are evaluated as:

(1) Cryptographic incident reports. See CMS-1A AMD-1, Ch9, Sect. 909.a(1-18).

(2) Personnel incident report. See CMS-1A AMD-1, Ch9, Sect. 909.b(1-6).

(3) Physical incident report. See CMS-1A AMD-1, Ch9, Sect. 909.c(1-21).

CUI

CMS-1A
AMD-1

THIS PAGE IS UNCLASSIFIED BUT MARKED "CONFIDENTIAL" FOR TRAINING PURPOSES ONLY

SAMPLE INITIAL REPORT OF COMSEC INCIDENT

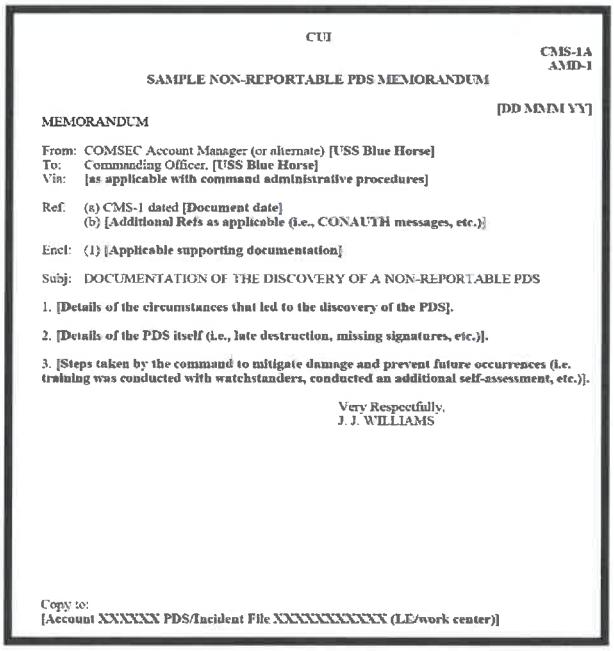
FM [USS GRAYWHALE]
TO [CONAUTH]
INFO DIRNSA FT GEORGE G MEADE MD (OMIT IF DIRNSA IS THE CA)
NCMS WASHINGTON DC
[ISIC]
[CHAIN OF COMMAND]
COMNAVRESFOR SUFFOLK VA
[SERVICING CMS AA TEAM]
ZEM
C O N F I D E N T I A L
MSGID/GENADMIN/[USS GRAYWHALE]/-/[MMM]//
SUBJ/INITIAL REPORT OF COMSEC INCIDENT//
REF/A/NCMS WASH DC/-/[DATE]//
AMPN/REF A IS CMS-1A//
POC/[XXXXXXXXXXXXX]/[RANK]/TEL/[(XXX)XXX-XXXX]/
EMAIL: [XXXXXXXXX(AT)XXXXXX.MIL]//
RMKS/IAW Ref A, the following is provided:
1. (U) [Account ######/HCI; Identify the COMSEC account number of the violating command or activity; if the violator is a LE of the account identified, state so here]
2. (U//CUI) [Short title, ED, Reg#, Classification, ALC, and CONAUTH if keying materiel]
3. (U//CUI) [List personnel involved (i.e., CAM, Radio Watchstander), Clearance level]
4. (C) [Detailed description of events surrounding the incident; if the report is IRT a tampered Mode 4/5 ECU, state whether tamper-evident protective technologies are present].
5. (U//CUI) [Physical, Cryptographic, or Personnel]
6. (U//CUI) [Corrective actions taken to mitigate damage and prevent future occurrences].
7. (U//CUI) [State whether a local investigation has been initiated and type].
8. (U) [State whether a damage assessment has been created OR NA].
9. (U) [(Initial reports) Indicate whether an SF-153 Relief from Accountability or Possession Report will be required. (Amplifying reports) Identify the transaction number of authorized RFA or possession reports].
10. (U) SAME AS POC ABOVE
11. (U) Additional data:
    A. (U) [Date of last COR Audit]
    B. (U) [Date of last completed self-assessment]
DERIVED FROM: NTISSI 4002//
DECL/[3 years from the DTG of the message]//
ZEN

Figure 7.1 LE COMSEC Incident Report

b. Timeframe for Reporting COMSEC Incidents, see below.

Materiel involved	Report Within	Message Precedence
Effective key, key which becomes effective within 15 days or any incidents involving espionage, subversion, defection, theft, tampering, clandestine exploitation, sabotage, hostile cognizant agent activity, or unauthorized copying, photographing or reproduction	24 hours	Immediate
Future key (becomes effective beyond 15 days from the date of the incident), superseded key, reserve on board or contingency key	48 hours	Priority
Any incident not covered by the above, i.e., loss of CCI equipment.	72 hours	Routine

7.2. Non-Reportable Practices Dangerous to Security (PDS). PDSs are reportable to the parent account and are practices, which potentially jeopardize the security of COMSEC material, if allowed to perpetuate. Non-Reportable PDSs will be documented and reported to the CO and the CNRFC KMI Team, as applicable no later than 72 hours from the time of discovery. See CMS-1A AMD-1, Ch10, Sect. 1003.a(1-41) for the full list of Non-Reportable PDSs.



CUI

CMS-1A
AMD-1

SAMPLE NON-REPORTABLE PDS MEMORANDUM

[DD MMM YY]

MEMORANDUM

From: COMSEC Account Manager (or alternate) [USS Blue Horse]
To: Commanding Officer, [USS Blue Horse]
Via: [as applicable with command administrative procedures]

Ref. (a) CMS-1 dated [Document date]
(b) [Additional Refs as applicable (i.e., CONAUTH messages, etc.)]

Encl: (1) [Applicable supporting documentation]

Subj: DOCUMENTATION OF THE DISCOVERY OF A NON-REPORTABLE PDS

1. [Details of the circumstances that led to the discovery of the PDS].

2. [Details of the PDS itself (i.e., late destruction, missing signatures, etc.)].

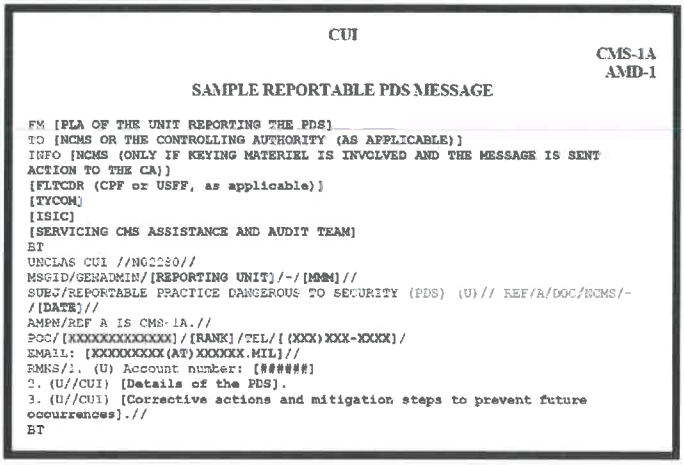
3. [Steps taken by the command to mitigate damage and prevent future occurrences (i.e. training was conducted with watchstanders, conducted an additional self-assessment, etc.)].

Very Respectfully,
J. J. WILLIAMS

Copy to:
[Account XXXXXX PDS/Incident File XXXXXXXXXXXX (LE/work center)]

Figure 7.2 Non-Reportable PDS example

7.3. Reportable Practices Dangerous to Security (PDS). PDSs are reportable to the parent account and are practices, which potentially jeopardize the security of COMSEC material, if allowed to perpetuate. Non-Reportable PDSs will be documented and reported to the CO and the CNRFC KMI Team, as applicable no later than 72 hours from the time of discovery. See CMS-1A AMD-1, Ch10, Sect. 1003.b(1-13) for the full list of Reportable PDSs. Figure 8.3 (below, will be followed and routed to the Local CO, ECH IV N6, and the CNRFC KMI Team.



CUI

CMS-1A
AMD-1

SAMPLE REPORTABLE PDS MESSAGE

FM [PLA OF THE UNIT REPORTING THE PDS]
TO [NCMS OR THE CONTROLLING AUTHORITY (AS APPLICABLE)]
INFO [NCMS (ONLY IF KEYING MATERIEL IS INVOLVED AND THE MESSAGE IS SENT ACTION TO THE CA)]
[FLTCDR (CPF or USFF, as applicable)]
[TYCOM]
[ISIC]
[SERVICING CMS ASSISTANCE AND AUDIT TEAM]
BT
UNCLAS CUI //N02280//
MSGID/GENADMIN/[REPORTING UNIT]/-/[MMM]//
SUBJ/REPORTABLE PRACTICE DANGEROUS TO SECURITY (PDS) (U)// REF/A/DOC/NCMS/-/[DATE]//
AMPN/REF A IS CMS-1A.//
POC/[XXXXXXXXXXXX]/[RANK]/TEL/[(XXX)XXX-XXXX]/
EMAIL: [XXXXXXXXX(AT)XXXXX.MIL]//
RMKS/1. (U) Account number: [######]
2. (U//CUI) [Details of the PDS].
3. (U//CUI) [Corrective actions and mitigation steps to prevent future occurrences].//
BT

Figure 7.3 Reportable PDS example

Note: All Reportable PDSs are required to be released via official naval message traffic.

Chapter 8

8.1. COMNAVRESFORCOM will provide cryptographic items and keying material to LE 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 an SF-153 inventory form.

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

Annex A - Definitions

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.

Commanding Officer - Individual ultimately responsible for the proper administration of their COMSEC material holdings and compliance with established KMI 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 Clerk - An individual assigned to assist COMSEC account personnel in the execution of certain administrative duties associated with the management of a COMSEC account.

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.

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

Crypto Equipment - Equipment that embodies a cryptographic logic (e.g., KG-175D).

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

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.

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

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 (HCI) - HCI 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 COMSEC matters for their subordinate commands.

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

KMI Client Node/Management Client (MGC) - 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 KMI Client Node is used by the COMNAVRESFORCOM KOA Manager.

KOA 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 KMI numbered account.

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

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

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

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

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

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(Hand Receipts). Retain for 90 days after the material has been destroyed, returned to the CAM or upon completion of the next LE inventory.

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. Inventory Report. Retain for 3 calendar years or until the next COR audit (the longer of the two).

e. Visitor Register. Retain for 1 year from the date the register has been completed or closed out.

f. Destruction Reports. Retain for 3 years calendar years or until the next COR audit (the longer of the two).

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

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

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

j. 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.

k. Trainings. Retain for 2 years reports of training stand downs, EAP/EDP drills, required reading, etc.

l. Spot Checks. CO/XO spot checks will be retained for two years or until completion of the next CMS COR audit.

m. Completed SF-701/702s. Retain for 30 days beyond the last date recorded on them.

n. SF-700 Monthly Inventory Log. Retain for one year or until the next COR audit, the sooner of the two.