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

COMNAVRESFORCOMINST 2280.1F
N64
8 Aug 2019

COMNAVRESFORCOM INSTRUCTION 2280.1F

From: Commander, Navy Reserve Forces Command

Subj: KEY MANAGEMENT INFRASTRUCTURE OPERATING ACCOUNT ADMINISTRATION AND MANAGEMENT PROCEDURES

Ref: (a) CMS-1
(b) CMS-3
(c) CMS-7
(d) SECNAVINST 5510.36A
(e) SECNAVINST 5510.30B
(f) KMI 5110 version 1

Encl: (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. This instruction is a complete revision and should be read in its entirety. This instruction is effective upon receipt.

2. Cancellation. COMNAVRESFORCOMINST 2280.1E.

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 contains enclosure (1). 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 (f). 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 177015 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 (f).

6. Action. Reserve Component Commanders (RCC), 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, shall be managed per Secretary of the Navy Manual M-5210.1, January 2012

9. Review and Effective Date. Per OPNAVINST 5215.17A, COMNAVRESFORCOM will review this instruction annually on the anniversary of its effective date to ensure applicability, currency, and consistency with Federal, DoD, SECNAV, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will automatically expire 5 years after effective date unless reissued or canceled prior to the 5-year anniversary date, or an extension has been granted.

T. W. LUSCHER

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/instructions.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 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, CMS-1, 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 Key Management Infrastructure (KMI) Team at CNRFC_EKMSTEAM@navy.mil.

COMNAVRESFORCOM
Key Management Infrastructure (KMI) Account Information

KMI Operating Account Number: 177015
Highest Classification Indicator: SECRET
Mailing Address:

COMNAVRESFORCOM
ATTN: KOA 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 KOA Manager or KMI team.

CNRF ISIC: (757)322-6646/DSN: 262-6646
KOA Manager: (757)322-6636/DSN: 262-6636
Alternate KOA Manager: (757)322-6638/DSN: 262-6638
COMSEC Account Clerk: (757)322-6638/DSN: 262-6638
COMNAVRESFORCOM SIPRNET Help: 1(757)322-6664

Record of Changes

CHANGE NUMBER IDENTIFICATION	DATE ENTERED (YYMMDD)	ENTERED BY (SIGNATURE) RANK/RATE

Table of Contents

Chapter 7

Chapter 8

Chapter 9

Chapter 10

Annex

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 Secret Internet Protocol Network (SIPRNet), KG-175D (TACLANE), and Secure Telephone Equipment (STE) phone.

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) 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. COMNAVRESFORCOM is assigned COMSEC 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 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). 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. The CO is responsible for properly administering his/her 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 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.

g. Local Element. LEs are separate entities or remote commands that receive COMSEC material and support from the COMNAVRESFORCOM COMSEC account. An entity is defined as internal to the command (i.e., SIPRNET Café, 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 KOA 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:

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-1 and CMS-3.

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 dropbox, LE may keep a local copy on hand.

(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 COMSEC compliance and deliverables to the KOA Manager. The RCC will consolidate reports and gather the status of assigned tasking for further submission to the KOA Manager. RCCs do not provide direction on the administration and management of LE COMSEC holdings.

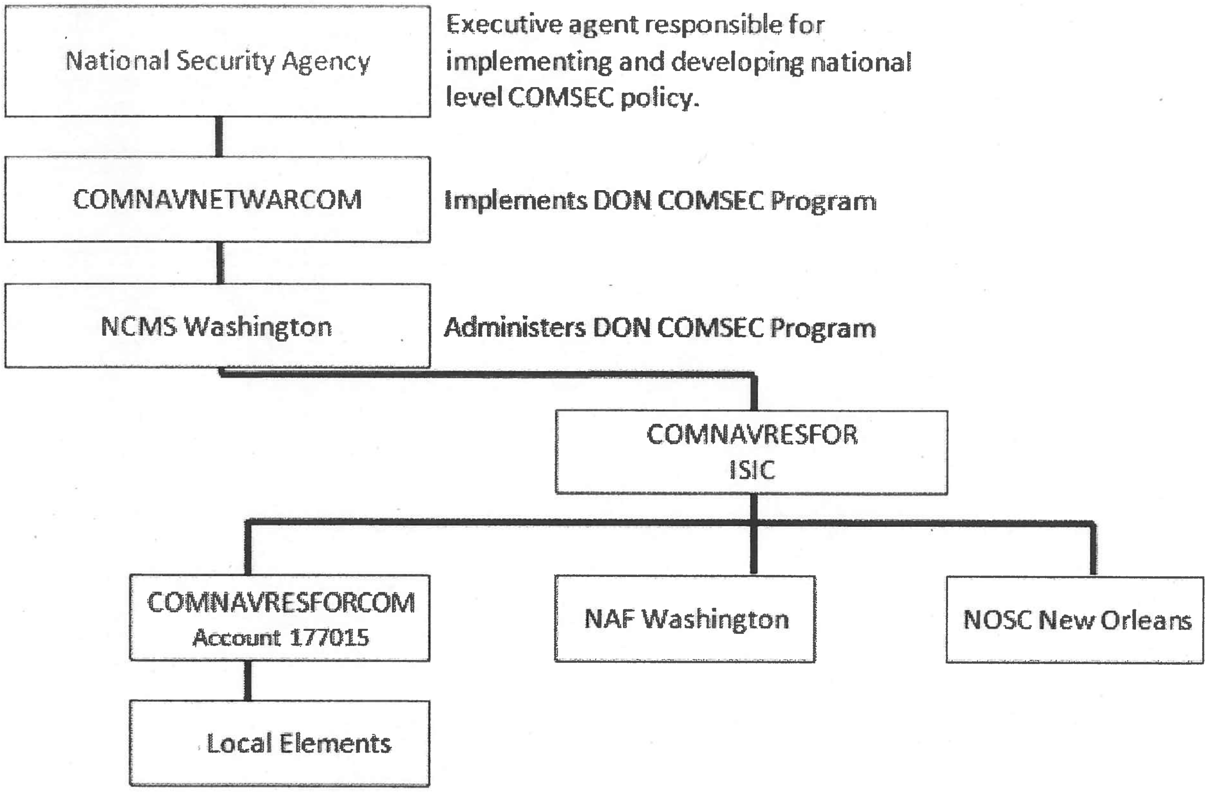

National Security Agency
Executive agent responsible for implementing and developing national level COMSEC policy.
COMNAVNETWARCOM
Implements DON COMSEC Program
NCMS Washington
Administers DON COMSEC Program
COMNAVRESFOR ISIC
COMNAVRESFORCOM Account 177015
NAF Washington
NOSC New Orleans
Local Elements

Figure 1.1 COMSEC Chain of Command

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 uncleared visitors as required. Uncleared visitors must be continuously escorted by a properly cleared person whose name is on the access list.

Note: 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 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.

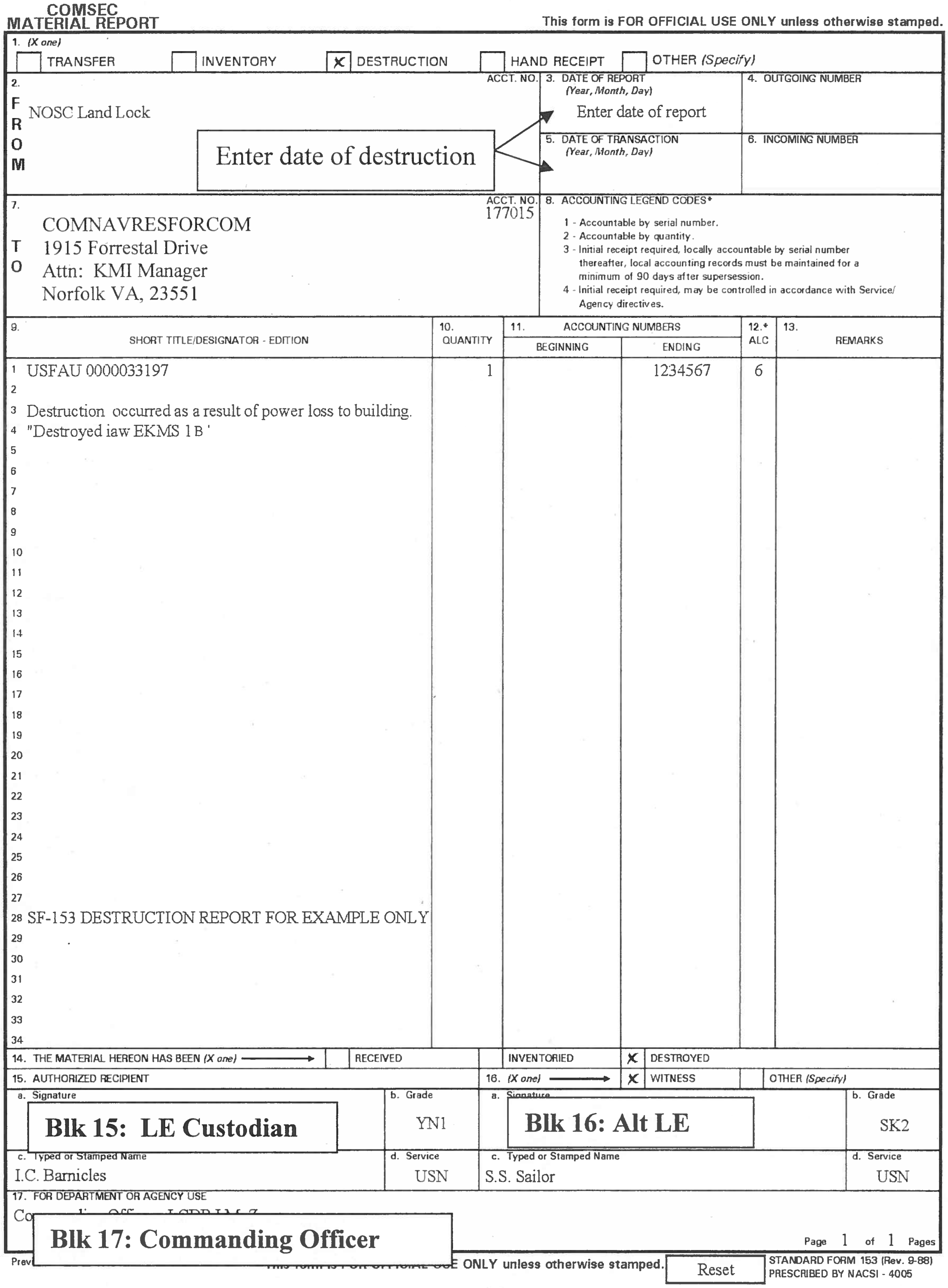
COMNAVRESFORCOM COMSEC personnel will provide monthly LE training and additional training as required. All LE Custodians are required to receive all training sessions.

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 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 KOA 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 Custodians (two person integrity). Authorization for destruction by LEs shall come from the parent command COMSEC 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 COMSEC account manager. See figure 3.1.



COMSEC MATERIAL REPORT

This form is FOR OFFICIAL USE ONLY unless otherwise stamped.

1. *(X one)* □ TRANSFER □ INVENTORY ☒ DESTRUCTION □ HAND RECEIPT □ OTHER *(Specify)*

2. FROM: NOSC Land Lock | ACCT. NO.

3. DATE OF REPORT *(Year, Month, Day)*: Enter date of report

4. OUTGOING NUMBER

5. DATE OF TRANSACTION *(Year, Month, Day)*

6. INCOMING NUMBER

Enter date of destruction

7. TO:
COMNAVRESFORCOM
1915 Forrestal Drive
Attn: KMI Manager
Norfolk VA, 23551

ACCT. NO. 177015

8. ACCOUNTING LEGEND CODES*
1 - Accountable by serial number.
2 - Accountable by quantity.
3 - Initial receipt required, locally accountable by serial number thereafter, local accounting records must be maintained for a minimum of 90 days after supersession.
4 - Initial receipt required, may be controlled in accordance with Service/Agency directives.

	9. SHORT TITLE/DESIGNATOR - EDITION	10. QUANTITY	11. ACCOUNTING NUMBERS BEGINNING	ENDING	12.* ALC	13. REMARKS
1	USFAU 0000033197	1		1234567	6	
2						
3	Destruction occurred as a result of power loss to building.					
4	"Destroyed iaw EKMS 1B '					
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28	SF-153 DESTRUCTION REPORT FOR EXAMPLE ONLY					
29						
30						
31						
32						
33						
34						

14. THE MATERIAL HEREON HAS BEEN *(X one)* → □ RECEIVED □ INVENTORIED ☒ DESTROYED

15. AUTHORIZED RECIPIENT | 16. *(X one)* → ☒ WITNESS □ OTHER *(Specify)*

a. Signature Blk 15: LE Custodian	b. Grade YN1	a. Signature Blk 16: Alt LE	b. Grade SK2
c. Typed or Stamped Name I.C. Barnicles	d. Service USN	c. Typed or Stamped Name S.S. Sailor	d. Service USN

17. FOR DEPARTMENT OR AGENCY USE
Co

Blk 17: Commanding Officer

Page 1 of 1 Pages

Prev

ONLY unless otherwise stamped. Reset

STANDARD FORM 153 (Rev. 9-88)
PRESCRIBED BY NACSI - 4005

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), Data Transfer Devices (DTDs), electronic keying material, KSV-21, 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 (e.g., 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 KOA Manager.

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. During an emergency condition, consider zeroizing all equipment and placing into a GSA approved space in your secure enclave.

Chapter 4

4.1 Secure Terminal Equipment. The STE is secure voice and data equipment that replaced the STU-III telephone. The security core is the KSV-21 cryptographic card which provides all security services. The KSV-21 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 will be issued to the LE command and signed for by the LE Custodian. The LE CO is solely responsible for safeguarding the KSV-21 and cannot transfer it to another individual without the authorization of the parent COMSEC 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 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 inserted may not be left unattended to prevent possible unauthorized use. However, the STE may be left unattended when the KSV-21 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 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. The unique serial number is used for accountability. The KSV-21 is classified as SECRET. When the KSV-21 is inserted into the telephone, the STE becomes

classified to the SECRET level. When the KSV-21 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 Key Support 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.

Chapter 5

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. Standard Form 153 (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 (Block 15), witness (Block 16).

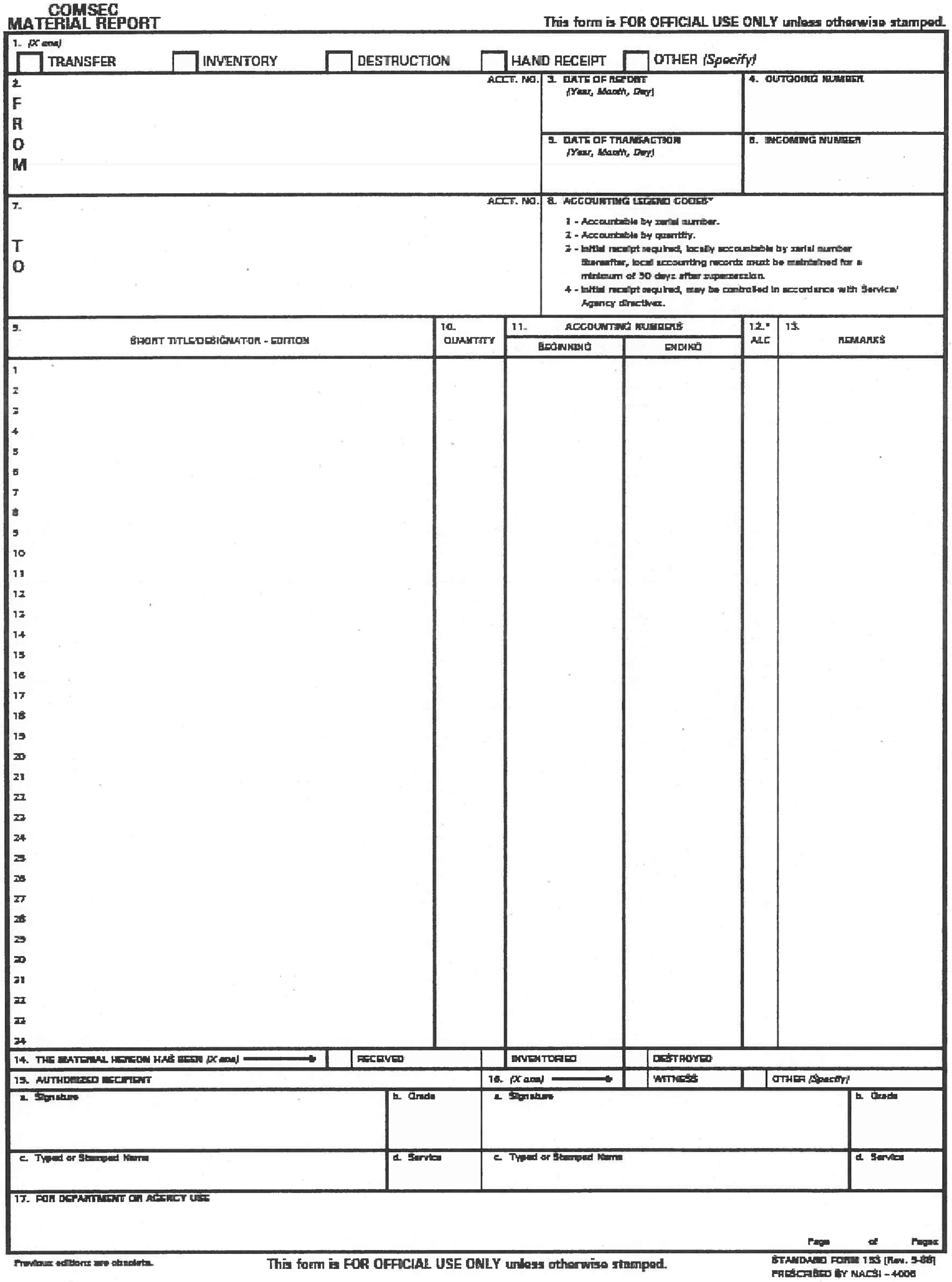
(2) "Inventory." Forward to LE to conduct physical inventory of COMSEC material.

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.



COMSEC
MATERIAL REPORT

This form is FOR OFFICIAL USE ONLY unless otherwise stamped.

1. *(X one)*
□ TRANSFER □ INVENTORY □ DESTRUCTION □ HAND RECEIPT □ OTHER *(Specify)*

2.
F
R
O
M

ACCT. NO.

3. DATE OF REPORT *(Year, Month, Day)*

4. OUTGOING NUMBER

5. DATE OF TRANSACTION *(Year, Month, Day)*

6. INCOMING NUMBER

7.
T
O

ACCT. NO.

8. ACCOUNTING LEGEND CODES*

1 - Accountable by serial number.
2 - Accountable by quantity.
3 - Initial receipt required, locally accountable by serial number thereafter, local accounting records must be maintained for a minimum of 30 days after supersession.
4 - Initial receipt required, may be controlled in accordance with Service/ Agency directives.

9. SHORT TITLE/DESIGNATOR - EDITION	10. QUANTITY	11. ACCOUNTING NUMBERS		12.* ALC	13. REMARKS
		BEGINNING	ENDING		
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					
24					

14. THE MATERIAL HEREON HAS BEEN *(X one)* → □ RECEIVED □ INVENTORIED □ DESTROYED

15. AUTHORIZED RECIPIENT

16. *(X one)* → □ WITNESS □ OTHER *(Specify)*

a. Signature	b. Grade	a. Signature	b. Grade
c. Typed or Stamped Name	d. Service	c. Typed or Stamped Name	d. Service

17. FOR DEPARTMENT OR AGENCY USE

Page of Pages

Previous editions are obsolete.

This form is FOR OFFICIAL USE ONLY unless otherwise stamped.

STANDARD FORM 153 (Rev. 5-88)
PRESCRIBED BY NACSI - 4006

Figure 5.1 SF-153 COMSEC Material Report

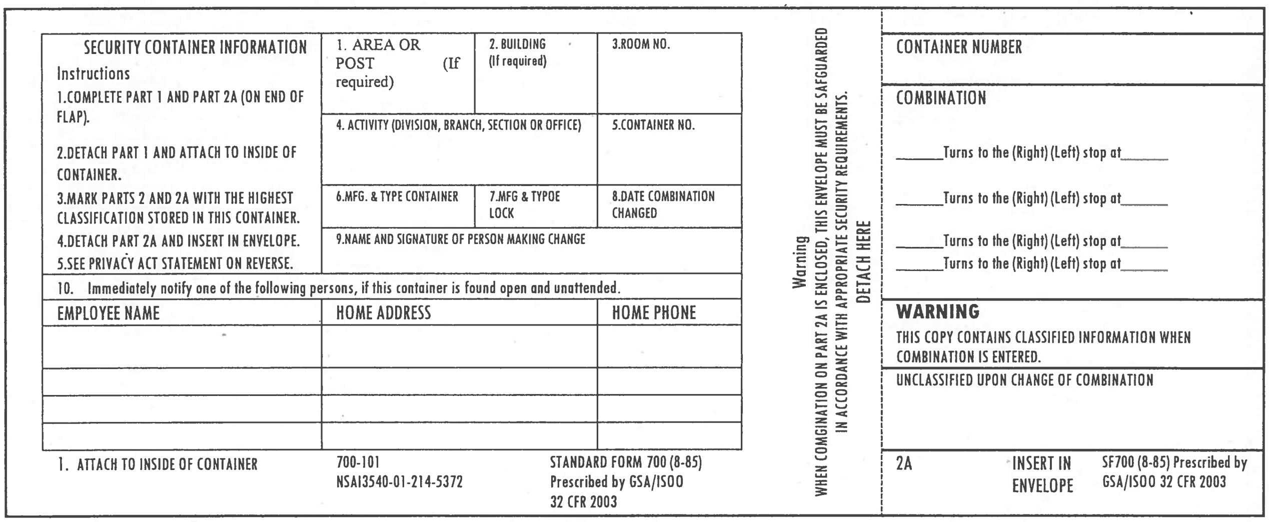
b. Standard Form 700 (SF-700) Security Container Information. Form SF-700 Security Container Information (figure 5.2) is used to maintain a record for each security container, vault or secure room door showing the location of each person by name, home address and home telephone number, having knowledge 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).



SECURITY CONTAINER INFORMATION Instructions 1.COMPLETE PART 1 AND PART 2A (ON END OF FLAP). 2.DETACH PART 1 AND ATTACH TO INSIDE OF CONTAINER. 3.MARK PARTS 2 AND 2A WITH THE HIGHEST CLASSIFICATION STORED IN THIS CONTAINER. 4.DETACH PART 2A AND INSERT IN ENVELOPE. 5.SEE PRIVACY ACT STATEMENT ON REVERSE.	1. AREA OR POST (If required)	2. BUILDING (If required)	3.ROOM NO.
	4. ACTIVITY (DIVISION, BRANCH, SECTION OR OFFICE)		5.CONTAINER NO.
	6.MFG. & TYPE CONTAINER	7.MFG & TYPOE LOCK	8.DATE COMBINATION CHANGED
	9.NAME AND SIGNATURE OF PERSON MAKING CHANGE		
10. Immediately notify one of the following persons, if this container is found open and unattended.			
EMPLOYEE NAME	HOME ADDRESS		HOME PHONE

1. ATTACH TO INSIDE OF CONTAINER

700-101
NSAI3540-01-214-5372

STANDARD FORM 700 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

Warning
WHEN COMGINATION ON PART 2A IS ENCLOSED, THIS ENVELOPE MUST BE SAFGUARDED IN ACCORDANCE WITH APPROPRIATE SECURITY REQUIREMENTS.
DETACH HERE

CONTAINER NUMBER

COMBINATION

______Turns to the (Right) (Left) stop at______

______Turns to the (Right) (Left) stop at______

______Turns to the (Right) (Left) stop at______
______Turns to the (Right) (Left) stop at______

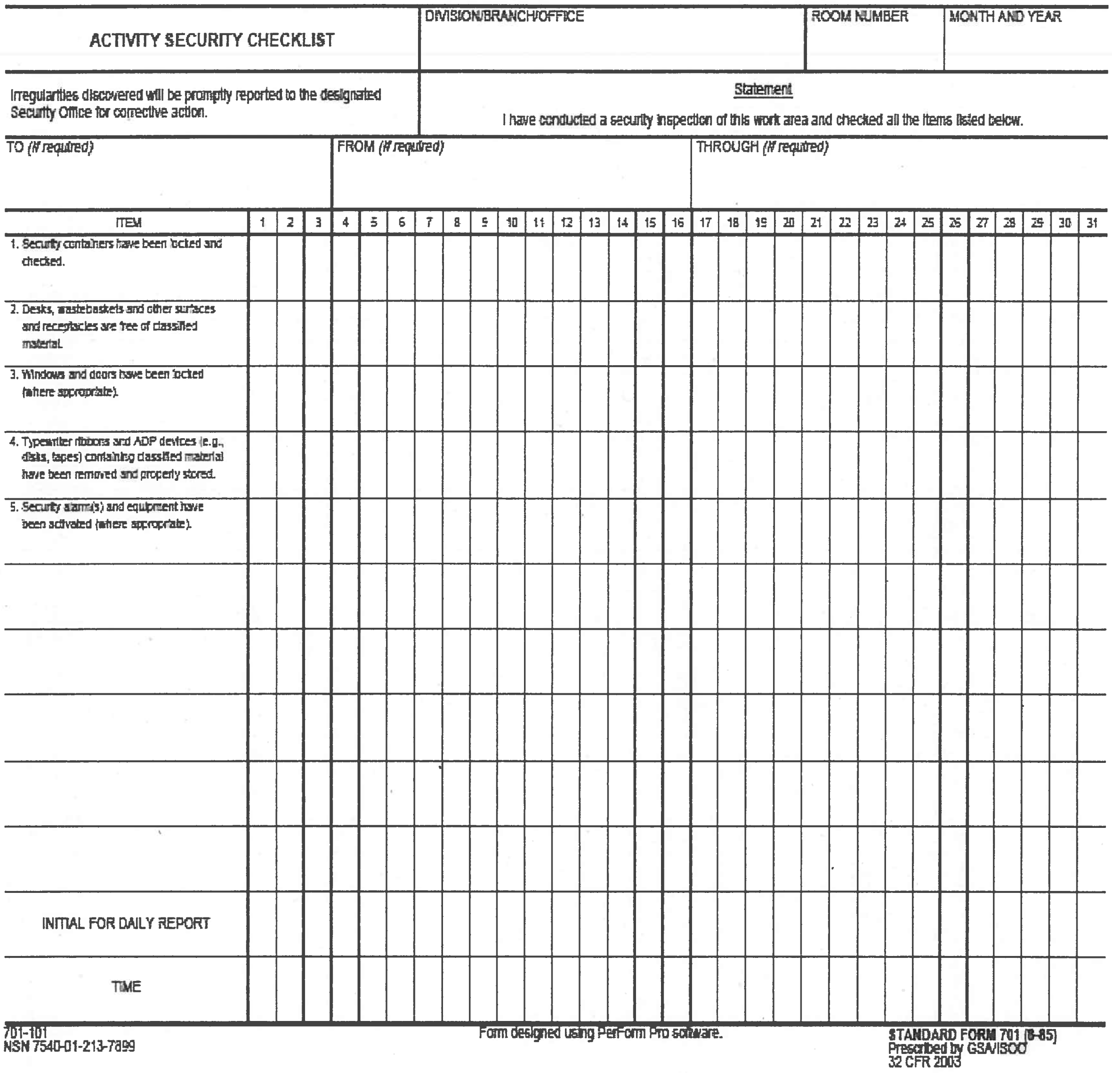
WARNING
THIS COPY CONTAINS CLASSIFIED INFORMATION WHEN COMBINATION IS ENTERED.

UNCLASSIFIED UPON CHANGE OF COMBINATION

2A INSERT IN ENVELOPE SF700 (8-85) Prescribed by GSA/ISOO 32 CFR 2003

Figure 5.2 SF-700 Security Container Information

c. Standard Form 701 (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.



ACTIVITY SECURITY CHECKLIST	DIVISION/BRANCH/OFFICE	ROOM NUMBER	MONTH AND YEAR
Irregularities discovered will be promptly reported to the designated Security Office for corrective action.	Statement I have conducted a security inspection of this work area and checked all the items listed below.		
TO *(If required)*	FROM *(If required)*	THROUGH *(If required)*	

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 locked and checked.																															
2. Desks, wastebaskets and other surfaces and receptacles are free of classified material.																															
3. Windows and doors have been locked (where appropriate).																															
4. Typewriter ribbons and ADP devices (e.g., disks, tapes) containing classified material have been removed and properly stored.																															
5. Security alarm(s) and equipment have been activated (where appropriate).																															
INITIAL FOR DAILY REPORT																															
TIME																															

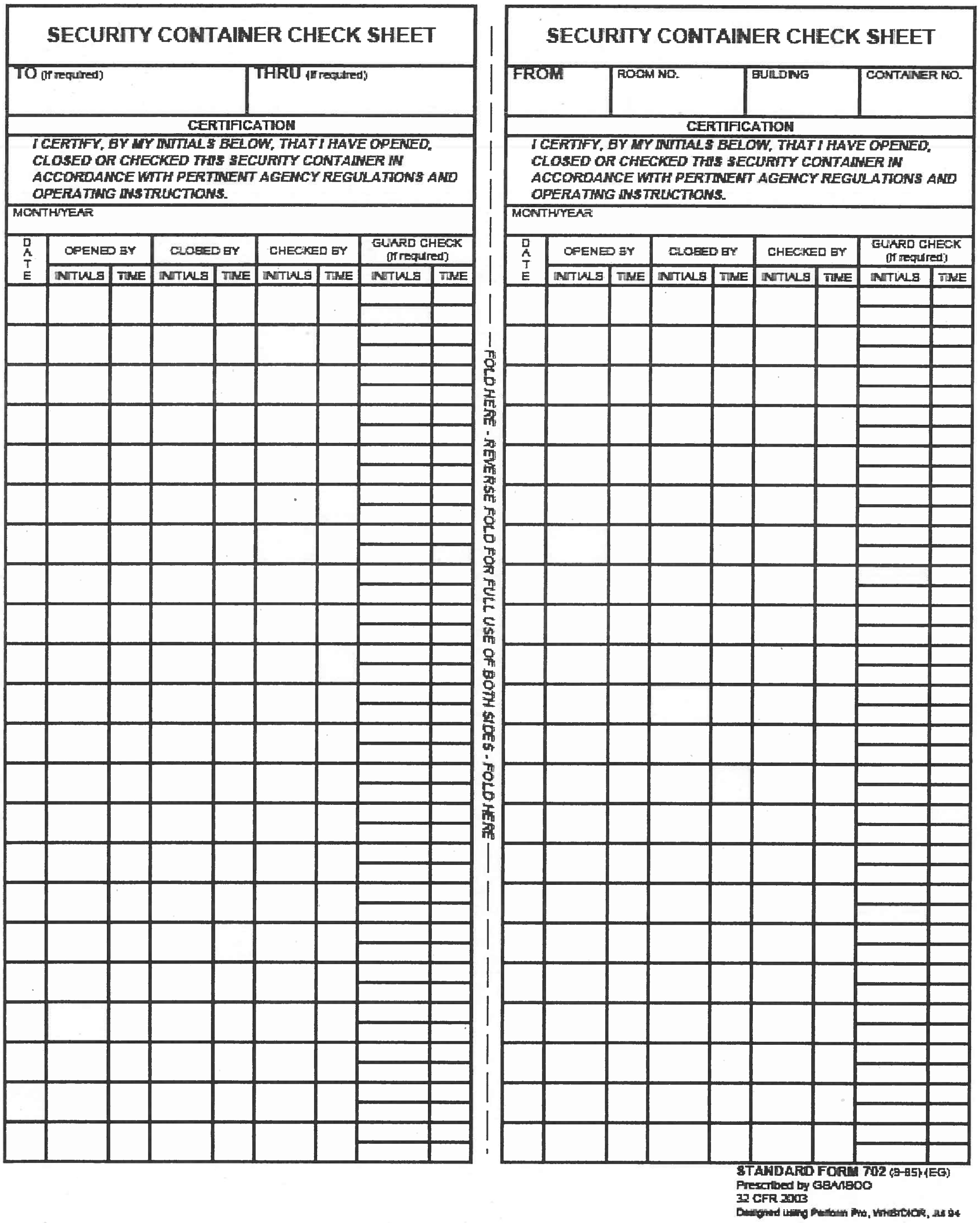
701-101
NSN 7540-01-213-7899

Form designed using PerForm Pro software.

STANDARD FORM 701 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

Figure 5.3 SF-701 Activity Security Check List

d. Standard Form 702 (SF-702) Security Container Check Sheet. Form SF-702 "Security Container Check Sheet" (Figure 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 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.



SECURITY CONTAINER CHECK SHEET

TO (If required)	THRU (If required)

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (If required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

FOLD HERE - REVERSE FOLD FOR FULL USE OF BOTH SIDES - FOLD HERE

SECURITY CONTAINER CHECK SHEET

FROM	ROOM NO.	BUILDING	CONTAINER NO.

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

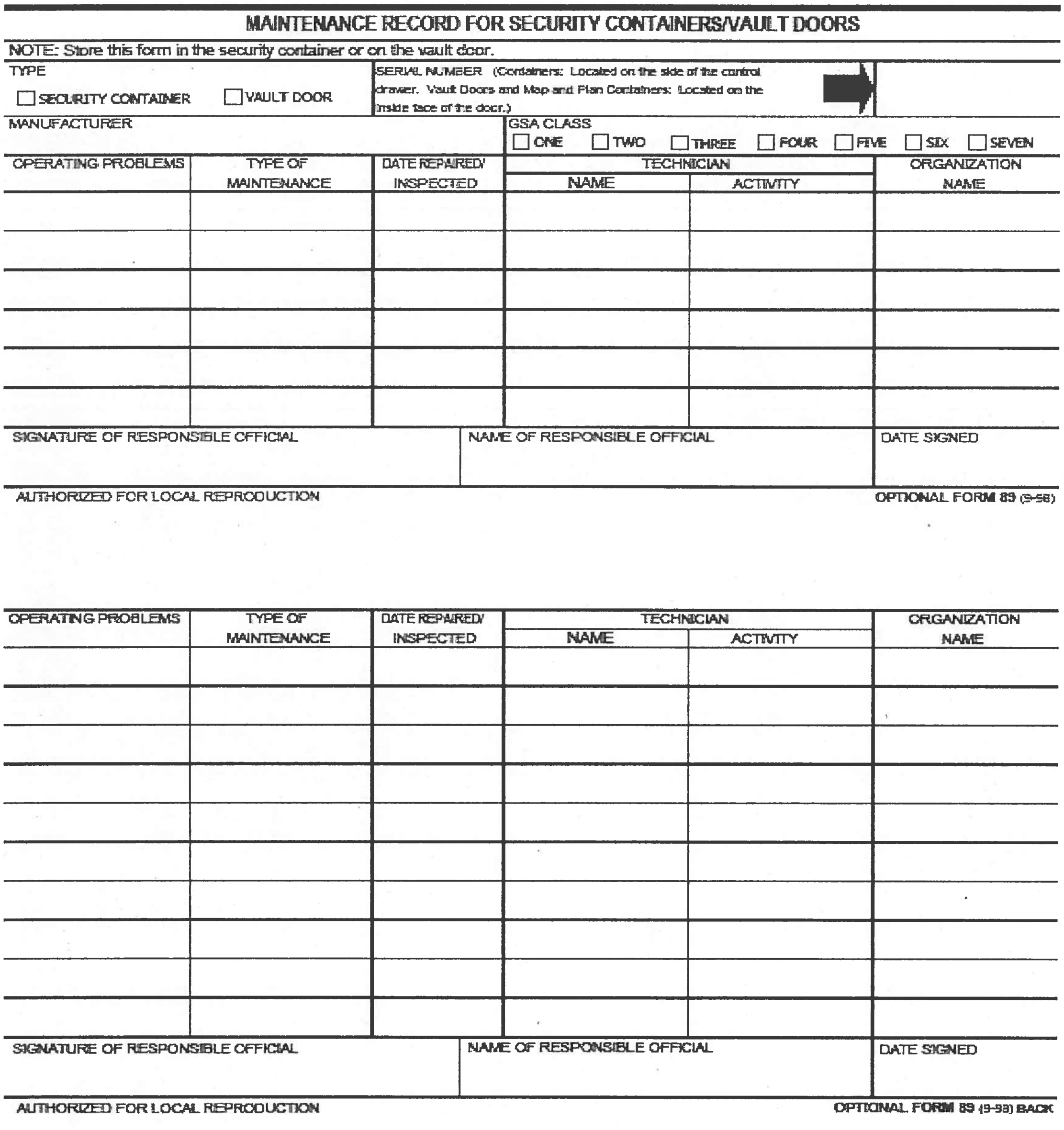
MONTH/YEAR

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (If required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

STANDARD FORM 702 (8-85) (EG)
Prescribed by GSA/ISOO
32 CFR 2003
Designed using Perform Pro, WHS/DIOR, Jul 94

Figure 5.4 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 5.5.



MAINTENANCE RECORD FOR SECURITY CONTAINERS/VAULT DOORS

NOTE: Store this form in the security container or on the vault door.

TYPE
□ SECURITY CONTAINER □ VAULT DOOR

SERIAL NUMBER (Containers: Located on the side of the control drawer. Vault Doors and Map and Plan Containers: Located on the inside face of the door.)

MANUFACTURER

GSA CLASS
□ ONE □ TWO □ THREE □ FOUR □ FIVE □ SIX □ SEVEN

OPERATING PROBLEMS	TYPE OF MAINTENANCE	DATE REPAIRED/ INSPECTED	TECHNICIAN		ORGANIZATION NAME
			NAME	ACTIVITY	

SIGNATURE OF RESPONSIBLE OFFICIAL	NAME OF RESPONSIBLE OFFICIAL	DATE SIGNED

AUTHORIZED FOR LOCAL REPRODUCTION
OPTIONAL FORM 89 (9-98)

OPERATING PROBLEMS	TYPE OF MAINTENANCE	DATE REPAIRED/ INSPECTED	TECHNICIAN		ORGANIZATION NAME
			NAME	ACTIVITY	

SIGNATURE OF RESPONSIBLE OFFICIAL	NAME OF RESPONSIBLE OFFICIAL	DATE SIGNED

AUTHORIZED FOR LOCAL REPRODUCTION
OPTIONAL FORM 89 (9-98) BACK

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

Chapter 6

6.1 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 E-MAIL.

6.2 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 6.1.

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 KSV-21 is placed in the phone or when the CIK is inserted in the KG-175D 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-175D, associated master and user keys) separately.

6.3 Receiving and Opening Communications Security Material Shipments

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

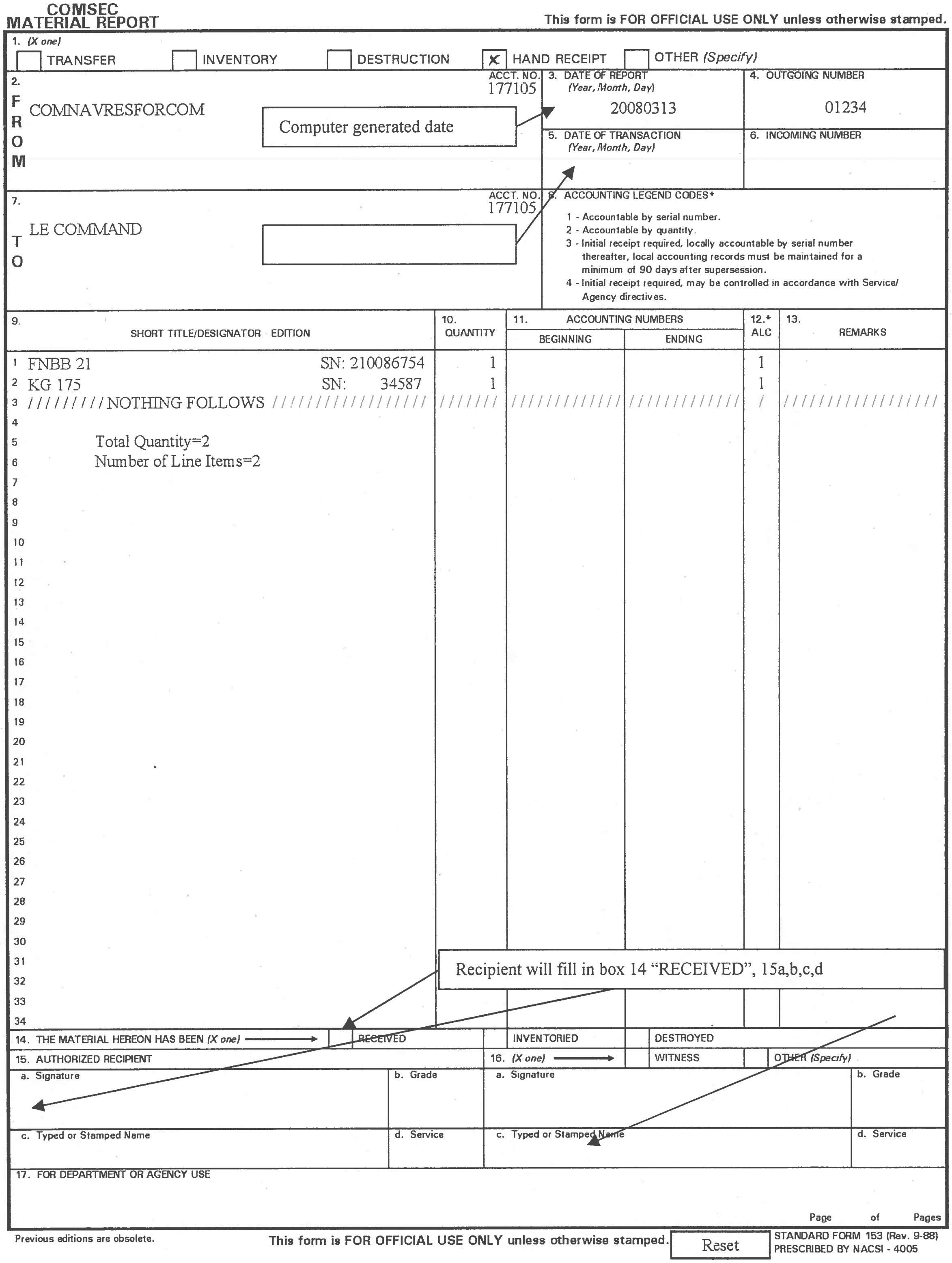
b. Open shipment.

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.



COMSEC
MATERIAL REPORT

This form is FOR OFFICIAL USE ONLY unless otherwise stamped.

1. *(X one)*
□ TRANSFER □ INVENTORY □ DESTRUCTION ☒ HAND RECEIPT □ OTHER *(Specify)*

2. FROM
COMNAVRESFORCOM

ACCT. NO. 177105

3. DATE OF REPORT *(Year, Month, Day)*
20080313

4. OUTGOING NUMBER
01234

Computer generated date

5. DATE OF TRANSACTION *(Year, Month, Day)*

6. INCOMING NUMBER

7. TO
LE COMMAND

ACCT. NO. 177105

8. ACCOUNTING LEGEND CODES*

1 - Accountable by serial number.
2 - Accountable by quantity.
3 - Initial receipt required, locally accountable by serial number thereafter, local accounting records must be maintained for a minimum of 90 days after supersession.
4 - Initial receipt required, may be controlled in accordance with Service/ Agency directives.

	9. SHORT TITLE/DESIGNATOR EDITION	10. QUANTITY	11. ACCOUNTING NUMBERS BEGINNING	ENDING	12.* ALC	13. REMARKS
1	FNBB 21 SN: 210086754	1			1	
2	KG 175 SN: 34587	1			1	
3	/////////NOTHING FOLLOWS //////////////////	///////	////////////	////////////	/	//////////////////
4						
5	Total Quantity=2					
6	Number of Line Items=2					
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						
32						
33						
34						

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

14. THE MATERIAL HEREON HAS BEEN *(X one)* → □ RECEIVED □ INVENTORIED □ DESTROYED

15. AUTHORIZED RECIPIENT
a. Signature
b. Grade
c. Typed or Stamped Name
d. Service

16. *(X one)* → □ WITNESS □ OTHER *(Specify)*
a. Signature
b. Grade
c. Typed or Stamped Name
d. Service

17. FOR DEPARTMENT OR AGENCY USE

Page of Pages

Previous editions are obsolete.

This form is FOR OFFICIAL USE ONLY unless otherwise stamped.

Reset

STANDARD FORM 153 (Rev. 9-88)
PRESCRIBED BY NACSI - 4005

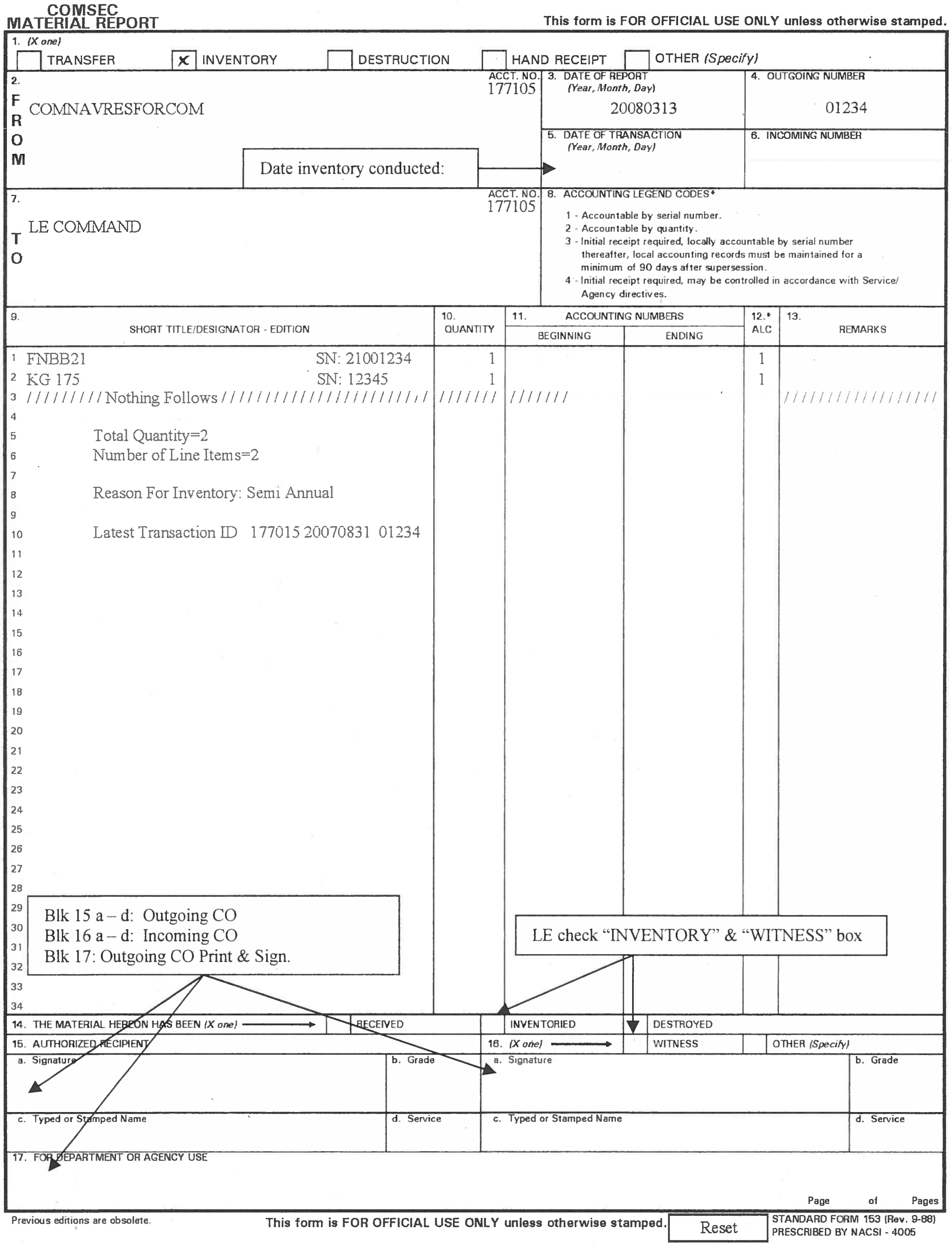
Figure 6.1 SF-153 Hand Receipt

Chapter 7

7.1 Communications Security Inventories

a. The parent COMSEC account 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 7.1 for an example of an SF-153 Inventory Report.

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



COMSEC
MATERIAL REPORT

This form is FOR OFFICIAL USE ONLY unless otherwise stamped.

1. *(X one)*
□ TRANSFER ☒ INVENTORY □ DESTRUCTION □ HAND RECEIPT □ OTHER *(Specify)*

2. FROM
COMNAVRESFORCOM

ACCT. NO. 177105

3. DATE OF REPORT *(Year, Month, Day)*
20080313

4. OUTGOING NUMBER
01234

5. DATE OF TRANSACTION *(Year, Month, Day)*

6. INCOMING NUMBER

Date inventory conducted:

7. TO
LE COMMAND

ACCT. NO. 177105

8. ACCOUNTING LEGEND CODES*
1 - Accountable by serial number.
2 - Accountable by quantity.
3 - Initial receipt required, locally accountable by serial number thereafter, local accounting records must be maintained for a minimum of 90 days after supersession.
4 - Initial receipt required, may be controlled in accordance with Service/ Agency directives.

	9. SHORT TITLE/DESIGNATOR - EDITION	10. QUANTITY	11. ACCOUNTING NUMBERS BEGINNING	ENDING	12.* ALC	13. REMARKS
1	FNBB21 SN: 21001234	1			1	
2	KG 175 SN: 12345	1			1	
3	/////////Nothing Follows///////////////////////	///////	///////			//////////////////
4						
5	Total Quantity=2					
6	Number of Line Items=2					
7						
8	Reason For Inventory: Semi Annual					
9						
10	Latest Transaction ID 177015 20070831 01234					
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						
30						
31						
32						
33						
34						

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

LE check "INVENTORY" & "WITNESS" box

14. THE MATERIAL HEREON HAS BEEN *(X one)* → □ RECEIVED □ INVENTORIED □ DESTROYED

15. AUTHORIZED RECIPIENT

a. Signature

b. Grade

c. Typed or Stamped Name

d. Service

16. *(X one)* → □ WITNESS □ OTHER *(Specify)*

a. Signature

b. Grade

c. Typed or Stamped Name

d. Service

17. FOR DEPARTMENT OR AGENCY USE

Page of Pages

Previous editions are obsolete.

This form is FOR OFFICIAL USE ONLY unless otherwise stamped.

Reset

STANDARD FORM 153 (Rev. 9-88)
PRESCRIBED BY NACSI - 4005

Figure 7.1 SF-153 COMSEC Inventory Report

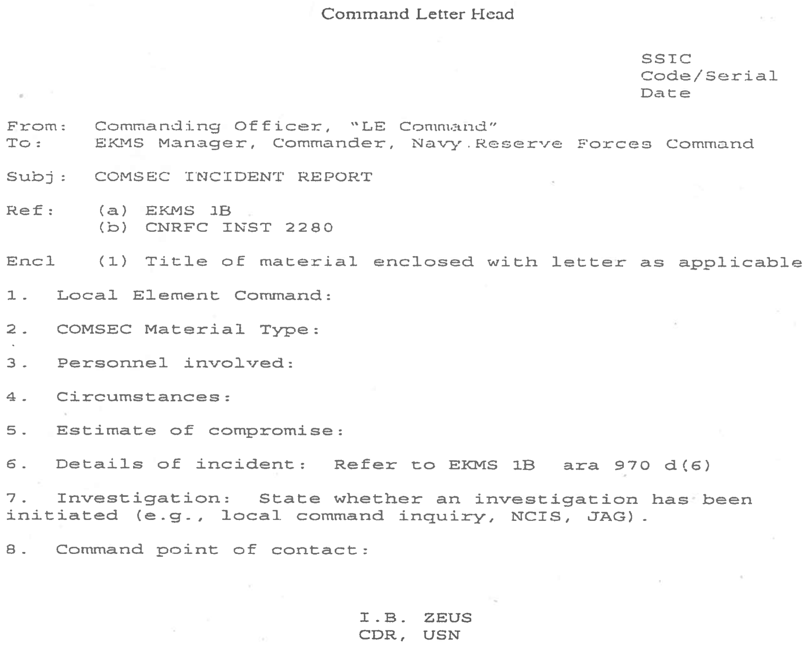
Chapter 8

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 KOA Manager. 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. 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 1B
(b) CNRFC INST 2280

Encl (1) Title of 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 1B ara 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

Chapter 9

9.1 Practices Dangerous to Security (PDS). PDSs 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. No change of command inventory conducted.

Command Letter Head

SSIC
Code/Serial
Date

From: Commanding Officer, "Local Element Command"
To: KMI Operating Account Manager, Commander, Navy Reserve Forces Command

Subj: PRACTICE DANGEROUS TO SECURITY

Ref: (a) CMS-1
(b) COMNAVRESFORCOMINST 2280.1E

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 (NMCI) Secret Internet Protocol Router (SIPR) Network. 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.

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.

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.

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 accounting 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 6: COMSEC material that is electronically generated and continuously accountable to the Central Office of Record from production to destruction.

AL 7: COMSEC material that is electronically generated and locally accountable to the COMNAVRESFORCOM KMI account.

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, KSV-21).

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

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.

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 KMI 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. 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 (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), (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.

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.

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.

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 conducted including 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. DD-2625. Retain for 90 days from the date the person no longer is assigned duties requiring the briefing.

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

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