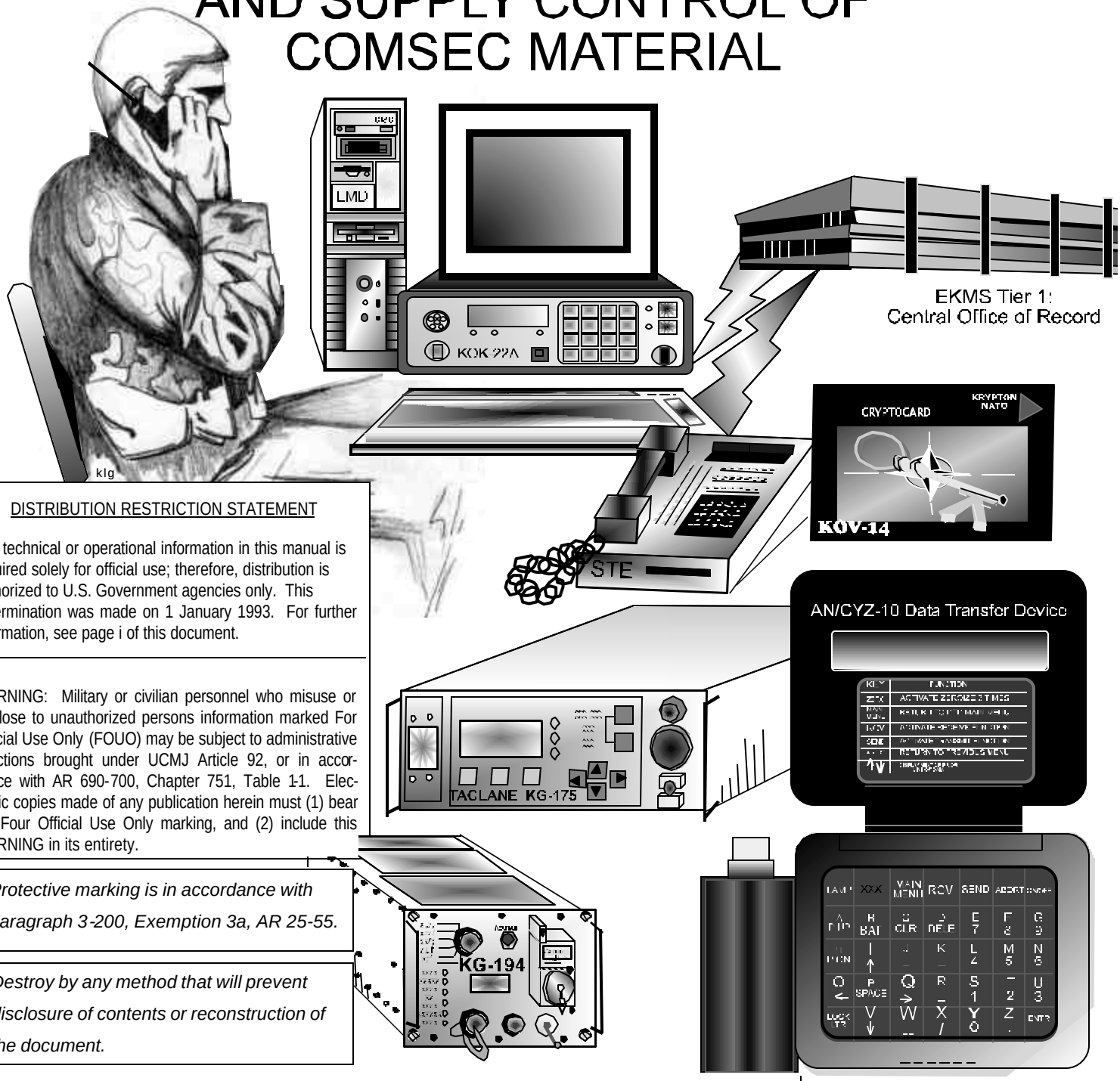
# TB 380-41

# TECHNICAL BULLETIN SECURITY: PROCEDURES FOR SAFEGUARDING, ACCOUNTING AND SUPPLY CONTROL OF COMSEC MATERIAL




DISTRIBUTION RESTRICTION STATEMENT

The technical or operational information in this manual is required solely for official use; therefore, distribution is authorized to U.S. Government agencies only. This determination was made on 1 January 1993. For further information, see page i of this document.

WARNING: Military or civilian personnel who misuse or disclose to unauthorized persons information marked For Official Use Only (FOUO) may be subject to administrative sanctions brought under UCMJ Article 92, or in accordance with AR 690-700, Chapter 751, Table 1-1. Electronic copies made of any publication herein must (1) bear the Four Official Use Only marking, and (2) include this WARNING in its entirety.

*Protective marking is in accordance with paragraph 3-200, Exemption 3a, AR 25-55.*

*Destroy by any method that will prevent disclosure of contents or reconstruction of the document.*


Headquarters, Department of the Army

Date of this Publication is 3 July 2003.

This bulletin supersedes TB 380-41, October 1994 and rescinds the use of DA Forms 2008 and 2009.


**FOR OFFICIAL USE ONLY**

DISTRIBUTION RESTRICTION STATEMENT

OUTSIDE THE U.S. GOVERNMENT RELEASE:

Requests from outside the U.S. Government for release of this publication under the Foreign Military Sales Program must be made to Commander, U.S. Army Security Assistance Center, ATTN: AMSAC-MI/I, 5002 Eisenhower Ave., Alexandria, VA 22333-0001. Request from outside the U.S. Government for release of this publication under the Freedom of Information Act must be made to the Director, Communications-Electronics Command (CECOM), Communications Security Logistics Activity (CSLA) at ATTN: SELCL-ID-P3, U.S. Army CECOM CSLA, 2133 Cushing Street, STE 3600, Fort Huachuca, AZ 85613-7041.

HEADQUARTERS
DEPARTMENT OF THE ARMY
Washington, D.C., 03 July 2003

# TECHNICAL BULLETIN

## SECURITY: PROCEDURES FOR SAFEGUARDING, ACCOUNTING AND SUPPLY CONTROL OF COMSEC MATERIAL

TB 380-41, July 2003, is changed from October 1994 as follows:
(Remove the old TB in its entirety and replace with the July 2003 edition.)

1. Added a chapter to address specific AKMS issues (Chapter 6).

2. Added a chapter specific to Incidents and their reporting (Chapter 7).

3. Included newer information about shredders.

4. Changed reporting time frames to cause all accounts to be the same (National Guard and Reserves still have an extension on time).

5. Added information on deployment issues.

6. Reduced the amount of samples and included more charts.

7. Eliminated the COMSEC account numbering system, as the account number no longer identifies the type of account.

8. Incorporated changes to the MARKS.

9. Incorporated ALC 6/7 key issues.

10. Eliminated specific issues concerning CLSFs, as they will no longer be handled differently from other accounts.

# TABLE OF CONTENTS

**Chapter/Paragraph** **Page**

CHAPTER 1 GENERAL ....1-1
1.1 PURPOSE .... 1-1
1.1.1 (U) Objective ....1-1
1.1.2 (U) Scope....1-1
1.1.3 (U) References, Abbreviations and Terms ....1-1

1.2 APPLICABILITY ....1-1

1.3 AVAILABILITY OF FORMS ....1-1

1.4 RESOLUTION OF CONFLICTS ....1-2

1.5 ARMY COMSEC WHOLESALE LOGISTICS MANAGEMENT PROGRAM ....1-2

1.6 COMMENTS AND RECOMMENDATIONS ....1-2

1.7 INTRODUCTION OF ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS) ....1-3

1.8 SERVICE AUTHORITY ....1-3

CHAPTER 2 COMSEC FACILITY, CMCS, ACCOUNTS, AND CUSTODIAN REQUIREMENTS .....2-1

2.1 COMSEC MATERIAL CONTROL SYSTEM (CMCS).... 2-1
2.1.1 (U) Army CMCS Structure ....2-3
2.1.2 (U) CMCS Addresses....2-5
2.1.3 (U) COMSEC Directory Service (formerly COMSEC Activity Address Directory.....2-6

2.2 COMSEC FACILITY .... 2-6
2.2.1 (U) Approving Office For the COMSEC Facility ....2-6
2.2.2 (U) COMSEC Facility Approvals ....2-6
2.2.3 (U) Request for Approval....2-7
2.2.4 (U) Action by Approving Authority ....2-7

2.3 ESTABLISHING A COMSEC ACCOUNT ....2-8

2.4 COMSEC ACCOUNT NUMBERING SYSTEM.... 2-8
2.4.1 (U) COMSEC Account Number/EKMS ID Structure....2-8
2.4.2 (U) Hand Receipt Numbers (Local Element) ....2-8

2.5 COMSEC ACCOUNT REGISTRATION PACKET (CARP).... 2-8
2.5.1 (U) COMSEC Account Registration Packet (CARP) Distribution....2-9
2.5.2 (U) Reporting COMSEC Account Data Changes ....2-9
2.5.3 (U) Completion of the CARP ....2-9
2.5.4 (U) Fund Code DODAAC ....2-9

2.6 SUPERVISION OF COMSEC FACILITIES ....2-11

2.7 COMSEC CUSTODIAN AND ALTERNATE REQUIREMENTS .... 2-11
2.7.1 (U) Custodian and Alternate Appointments ....2-11
2.7.2 (U) Custodian/Alternate and Witness Duties ....2-12

**Chapter/Paragraph** **Page**

2.8 COMSEC CUSTODIAN ABSENCE ....2-14

2.9 RELIEF FROM ACCOUNTABILITY ....2-15

2.10 MOVEMENT OF COMSEC ACCOUNTS .... 2-15
2.10.1 (U) Traditional Account Custodian Actions ....2-15
2.10.2 (U) AKMS Account Custodian Actions ....2-16
2.10.3 (U) COR Processing Actions ....2-16

2.11 CLOSING OF COMSEC ACCOUNTS .... 2-16
2.11.1 (U) Commander's Actions ....2-16
2.11.2 (U) COR Procedures Upon Closure of COMSEC Accounts ....2-17
2.11.3 (U) Closing of Accounts Due to Inactivity ....2-17

2.12 CONTINGENCY DEPLOYMENT OF A COMSEC ACCOUNT....2.17
2.12.1 (U) Traditional COMSEC Account Contingency Deployment....2.17
2.12.2 (U) AKMS COMSEC Account Contingency Deployment....2.18
2.12.3 (U) Additional Requirements for Deploying COMSEC Accounts....2.18
2.12.4 (U) CSLA Responsibilities to the Deployed Account....2.19

2.13 UNIT DEPLOYMENT WITHOUT COMSEC ACCOUNTS .... 2-19
2.13.1 (U) Mission Support ....2-19
2.13.2 (U) Suspension of a COMSEC Account ....2-19
2.13.3 (U) Unit Return to Home Station ....2-20
2.13.4 (U) CSLA Responsibilities for a Suspended Account ....2-21

CHAPTER 3 SUPPLY AND CONTROLLING AUTHORITY PROCEDURES ....3-1

3.1 IDENTIFYING COMSEC MATERIAL ....3-1

3.2 REQUISITION FUNDING AND RETURNS .... 3-1
3.2.1 (U) Requisitions ....3-1
3.2.2 (U) Customer Returns ....3-2
3.2.3 (U) Customer Assistance....3-3

3.3 REQUISITIONING OF COMSEC MATERIAL .... 3-3
3.3.1 (U) General COMSEC Requisition Procedures and Applicable Publications....3-3
3.3.2 (U) Initial Issue of COMSEC Publications ....3-3
3.3.3 (U) Identification Plates/Labels ....3-4
3.3.4 (U) Equipment Alteration ....3-5

3.4 NEED FOR CRYPTOSYSTEMS AND AUTHENTICATION SYSTEMS.... 3-5
3.4.1 (U) Information Security ....3-5
3.4.2 (U) Authentication Systems ....3-5
3.4.3 (U) Operations Security (OPSEC)....3-5
3.4.4 (U) Approved Systems ....3-5
3.4.5 (U) Selection and Use ....3-5

3.5 CRYPTONETS .... 3-5
3.5.1 (U) Cryptonet Elements....3-5
3.5.2 (U) Types of Cryptonets ....3-6
3.5.3 (U) Cryptonet Size ....3-6
3.5.4 (U) Cryptonet Expansion ....3-6

**Chapter/Paragraph** **Page**

3.6 ESTABLISHMENT OF CRYPTONETS ..... 3-6
3.6.1 (U) Requests for Key Tapes ..... 3-10
3.6.2 (U) AKMS Accounts ..... 3-13
3.6.3 (U) Requests to Hold Other Services or Agencies Cryptonets Key ..... 3-13
3.6.4 (U) Requests for Foreign Release ..... 3-13

3.7 CONTROLLING AUTHORITY ..... 3-13
3.7.1 (U) Management Responsibilities ..... 3-13
3.7.2 (U) Operational Responsibilities ..... 3-14
3.7.3 (U) Logistics Support ..... 3-15
3.7.4 (U) Key Material Compromises ..... 3-16
3.7.5 (U) Defective Keying Material ..... 3-17
3.7.6 (U) Key Material Reviews ..... 3-17
3.7.7 (U) Designating Contingency Keying Material ..... 3-18
3.7.8 (U) Disposition Instructions for Keying Material ..... 3-18

3.8 COMSEC KEY ..... 3-18
3.8.1 (U) Authorization to Receive COMSEC Key ..... 3-18
3.8.2 (U) Establishing Cryptonets and Initial Issue of COMSEC Key Material ..... 3-18
3.8.3 (U) Shipment of Physical COMSEC Key ..... 3-18
3.8.4 (U) Transfer Reports for COMSEC Key ..... 3-18
3.8.5 (U) Excess and Unserviceable COMSEC Key ..... 3-18
3.8.6 (U) Resupply Procedures for COMSEC Key ..... 3-18
3.8.7 (U) Processing Requests ..... 3-19
3.8.8 (U) Classification ..... 3-19

3.9 DETERMINING COPY COUNT REQUIREMENTS ..... 3-23
3.9.1 (U) Excessive Use of Manual and Auto-manual Cryptosystems ..... 3-23
3.9.2 (U) Rapid Net Expansion ..... 3-23

3.10 USER HOLDINGS OF KEY MATERIAL ..... 3-23
3.10.1 (U) Amount of Key to be Held by COMSEC Accounts ..... 3-23
3.10.2 (U) Number of Holders/Pages Per System ..... 3-23
3.10.3 (U) Joint/Combined Operations ..... 3-23
3.10.4 (U) Exceptions ..... 3-23
3.10.5 (U) Amount of Key Issued to Users ..... 3-24

3.11 EMERGENCY REQUIREMENTS FOR KEY ..... 3-24

CHAPTER 4 ACCOUNTING AND REPORTING PROCEDURES ..... 4-1

4.1 GENERAL ..... 4-1

4.2 COMSEC MATERIAL ACCOUNTING LEGEND CODES (ALC) ..... 4-2

4.3 FILES, FORMS AND REPORTS ..... 4-2
4.3.1 COMSEC Accounting Reports Guide ..... 4-4

4.4 RECEIPT INSPECTION AND INVENTORY OF COMSEC MATERIAL ..... 4-8
4.4.1 (U) General ..... 4-8
4.4.2 (U) TOP SECRET Key ..... 4-8
4.4.3 (U) Package/Container Examination ..... 4-8
4.4.4 (U) Transfer Reports SF 153 ..... 4-8
4.4.5 (U) Page Checking Keying Material ..... 4-9

**Chapter/Paragraph.....Page**

4.4.6 (U) Page Checking COMSEC Publications (KAM, KAO, ETC,) .....4-9
4.4.7 (U) Inventory of Sealed Material, Packages and Shipping Containers .....4-9

4.5 ASSIGNMENT OF COMSEC MATERIAL VOUCHER NUMBERS .....4-10

4.6 PREPARATION OF VOUCHER CONTROL REGISTER (DA Form 4669-E)..... 4-12
4.6.1 (U) Use of DA Form 4669-E.....4-12
4.6.2 (U) DA Form 4669-E Completion Instructions .....4-12

4.7 ITEM REGISTER (IR) CARDS……4-14
4.7.1 (U) General Instructions .....4-14
4.7.2 (U) DA Form 2011-E COMSEC Aids Items Register.....4-14
4.7.3 (U) DA Form 2011-1-E COMSEC Equipment Items Register.....4-17

4.8 CONTROL OF KEY TAPE SEGMENTS ..... 4-21
4.8.1 (U) Digraph Code for COMSEC Key .....4-21
4.8.2 (U) Local Accounting for COMSEC Key .....4-21
4.8.3 (U) Authorized Exposure of Keying Material .....4-23

4.9 PREPARATION OF COMSEC MATERIAL REPORT (SF 153) ..... 4-26
4.9.1 (U) General .....4-26
4.9.2 (U) SF 153 General Completion Instructions .....4-26

4.10 TRANSFER OF COMSEC MATERIAL..... 4-31
4.10.1 (U) Transfer of COMSEC Material Between COMSEC Accounts .....4-31
4.10.2 (U) Responsibilities ..... 4-31

4.11 LOCAL ACCOUNTING FOR COMSEC MATERIAL..... 4-31
4.11.1 (U) Responsibilities .....4-31
4.11.2 (U) ALC 1 and 2 COMSEC Material .....4-31
4.11.3 (U) Hand Receipting COMSEC Material .....4-32

4.12 INVENTORY REQUIREMENTS FOR COMSEC MATERIAL..... 4-34
4.12.1 (U) Inventory Requirements for COMSEC Accounts.....4-34
4.12.2 (U) CLSF Inventory Procedures .....4-35
4.12.3 (U) Daily and Shift-to-Shift Inventory of Key Material .....4-35

4.13 REPORTING PROCEDURES FOR INVENTORIES ..... 4-39
4.13.1 (U) COMSEC Account Semiannual Inventory Report (SAIR) for Traditional (Manual) Accounts .....4-39
4.13.2 (U) COMSEC Account Semiannual Inventory Report (SAIR) for AKMS Accounts.....4-42
4.13.3 (U) COMSEC Account Change of Custodian Inventory Report (CCIR) for Traditional Accounts .....4-42
4.13.4 (U) COMSEC Account Change of Custodian Inventory Report (CCIR) for AKMS Accounts.....4-43
4.13.5 (U) Inventory of ALC 4 COMSEC Material .....4-43
4.13.6 (U) Procedures to Change Alternate Custodians .....4-44
4.13.7 (U) Special Inventory Report.....4-44

4.14 CONVERSION AND SPECIAL POSSESSION REPORTS ..... 4-44
4.14.1 (U) Conversion Report .....4-44
4.14.2 (U) Special Possession Report .....4-45

**Chapter/Paragraph.....Page**

4.15 ACCOUNTING FOR AND ENTERING AMENDMENTS TO COMSEC PUBLICATIONS ..... 4-45
4.15.1 (U) Interim Amendments .....4-45
4.15.2 (U) Reproductions of Interim Amendments .....4-45
4.15.3 (U) Official Amendments .....4-45

4.16 ACCOUNTING FOR ALC 4 MATERIAL .....4-46

4.17 REPRODUCTION OF COMSEC MATERIAL ..... 4-47
4.17.1 (U) Accountable Publications .....4-48
4.17.2 (U) Destruction of Reproducible Extracts .....4-48
4.17.3 (U) Publications Prohibiting Reproduction .....4-48

4.18 MODIFICATION AND FABRICATION OF COMSEC MATERIAL .....4-49

4.19 DESTRUCTION OF COMSEC MATERIAL ..... 4-49
4.19.1 (U) Routine Destruction Procedures .....4-49
4.19.2 (U) Scheduled Destruction .....4-50
4.19.3 (U) Destruction Procedures .....4-51
4.19.4 (U) Destruction of Paper-Based and Keying Material (& Mylar Key Tape) .....4-51
4.19.5 (U) Destruction of Other COMSEC Material .....4-53
4.19.6 (U) Destruction of Accountable COMSEC Material On Hand Receipts .....4-53

4.20 AUDIT/INSPECTION OF COMSEC ACCOUNTS ..... 4-54
4.20.1 (U) Basis for Audit .....4-54
4.20.2 (U) Notification of Audit .....4-54
4.20.3 (U) Scope of the Audit .....4-54
4.20.4 (U) Suggested Local Pre-Inspection Checklist .....4-55
4.20.5 (U) Audit Report .....4-55

CHAPTER 5 SAFEGUARDING COMSEC MATERIAL .....5-1

5.1 GENERAL .....5-1

5.2 CLASSIFICATION GUIDELINES FOR COMSEC INFORMATION ..... 5-1
5.2.1 (U) Foreign Release .....5-1
5.2.2 (U) Handling and Release of Unclassified COMSEC Information .....5-1
5.2.3 (U) FOR OFFICIAL USE ONLY Application .....5-1
5.2.4 (U) Compilations .....5-2
5.2.5 (U) Use of Caveat “CRYPTO” .....5-2
5.2.6 (U) Marking of COMSEC Equipment .....5-2
5.2.7 (U) Controlled Cryptographic Items (CCI) .....5-3
5.2.8 (U) COMSEC Classification Guidance .....5-3
5.2.9 (U) Classification Duration .....5-3

5.3 PHYSICAL SECURITY MEASURES .....5-3

5.4 ACCESS TO AND IDENTIFICATION OF COMSEC FACILITY .....5-4

5.5 PROTECTION OF FIXED COMSEC FACILITIES .....5-5
5.5.1 (U) Installation of On-Line Crypto-equipment .....5-5
5.5.2 (U) Secure Room Operations .....5-5
5.5.3 (U) General Area Operations .....5-5
5.5.4 (U) Devices (other than COMEC equipment) Used Within a COMSEC Facility .....5-5
5.5.5 (U) Electronic Access Control Devices .....5-5

**Chapter/Paragraph** **Page**

5.6 SECURITY CHECKS ....5-6
5.6.1 (U) Types of Security Checks ....5-6
5.6.2 (U) Area Security ....5-6

5.7 PROTECTION OF MOBILE AND TRANSPORTABLE COMSEC FACILITIES .... 5-6
5.7.1 (U) Protection ....5-7
5.7.2 (U) Minimum Mobile COMSEC Facility Protection ....5-7

5.8 USE OF GUARDS ....5-7

5.9 EMPLOYMENT OF COMSEC EQUIPMENT AT UNATTENDED SITES ....5-8

5.10 STORAGE OF COMSEC MATERIAL....5-8
5.10.1 (U) Storage of Classified CRYPTO Key ....5-8
5.10.2 (U) Storage of Unclassified CRYPTO Key ....5-9
5.10.3 (U) Storage Restrictions ....5-9
5.10.4 (U) Storage of COMSEC Equipment and Components ....5-10

5.11 TRANSPORTATION OFCOMSEC MATERIAL ....5-12

5.12 KEYING MATERIAL MARKED “CRYPTO” ....5-12
5.12.1 (U) Preparation for Shipment ....5-12
5.12.2 (U) Methods of Shipment....5-13

5.13 COMSEC EQUIPMENT AND COMPONENTS .... 5-13
5.13.1 (U) Use of U.S. Commercial Passenger Airlines....5-13
5.13.2 (U) Protecting Classified COMSEC Equipment While in Transportation Channels ....5-14
5.13.3 (U) Packaging ....5-15
5.13.4 (U) Contents Identification ....5-15

5.14 CRYPTOLOGIC MEDIA ....5-16

5.15 SHIPMENT OF CLASSIFIED WITH UNCLASSIFIED COMSEC MATERIAL....5-16

5.16 COURIERS .... 5-16
5.16.1 (U) Courier Requirements ....5-16
5.16.2 (U) Courier Responsibilities ....5-17
5.16.3 (U) Airdrop of COMSEC Material ....5-17

5.17 EMERGENCY PLANS AND PROCEDURES ....5-17

5.18 PREPARATION OF EMERGENCY PLANS .... 5-18
5.18.1 (U) Provisions ....5-18
5.18.2 (U) Coordination ....5-19

5.19 RECOMMENDED EMERGENCY TASK CARDS .... 5-19
5.19.1 (U) Task Cards ....5-19
5.19.2 (U) Sample Task Cards ....5-19

5.20 EMERGENCY MEASURES .... 5-19
5.20.1 (U) Emergency Evacuation ....5-19
5.20.2 (U) Secure Storage During an Emergency....5-19
5.20.3 (U) Emergency Destruction ....5-20
5.20.4 (U) Priorities ....5-20

**Chapter/Paragraph.....Page**

5.21 EMERGENCY DESTRUCTION METHODS AND MATERIALS..... .....5-20
5.21.1 (U) Key and COMSEC Documents .....5-20
5.21.2 (U) Shredders.....5-20
5.21.3 (U) Sodium Nitrate Destructors .....5-21
5.21.4 (U) Destruction of COMSEC Equipment .....5-24
5.21.5 (U) Destruction in Aircraft .....5-26

5.22 DESTRUCTION OF COMSEC MAINTENANCE MANUALS .....5-26

5.23 ACTIONS AFTER AN EMERGENCY .....5-27

5.24 PRECAUTIONARY ACTIONS .....5-28

CHAPTER 6 ARMY KEY MANAGEMENT SYSTEM (AKMS) .....6-1

6.1 GENERAL..... 6-1
6.1.1 (U) Primary Tier 1 Sites (PT1S) .....6-1

6.2 LOCAL COMSEC MANAGEMENT SOFTWARE (LCMS) WORKSTATION ..... 6-1
6.2.1 (U) Purpose .....6-1
6.2.2 (U) LCMS Workstation.....6-1
6.2.3 (U) LCMS Functional Elements .....6-1
6.2.4 (U) LCMS Power Requirements .....6-2

6.3 ACCOUNTABILITY OF THE LCMS WORKSTATION.....6-2

6.4 INVENTORY REQUIREMENTS ..... 6-2
6.4.1 (U) COMSEC Account Semiannual Inventory Report (SAIR) .....6-2
6.4.2 (U) COMSEC Account Change of Custodian Inventory Report (CCIR) .....6-2
6.4.3 (U) Special Inventory Report (SIR).....6-3
6.4.4 (U) Change of Account Location Inventory Report.....6-3
6.4.5 (U) AKMS Daily and Shift Change Inventory Requirements .....6-3
6.4.6 (U) ALC 4 Inventory Requirements .....6-3

6.5 LOCAL ACCOUNTING FOR COMSEC MATERIAL..... 6-5
6.5.1 (U) Hand Receipts (HR).....6-5
6.5.2 (U) Inventory Maintenance .....6-5
6.5.3 (U) Accounting for Superseded Key .....6-5
6.5.4 (U) Issue of ALC 4 Material Within AKMS.....6-6
6.5.5 (U) Clearing Typographical Errors (in LCMS).....6-6
6.5.6 (U) Recording STU-III Key Conversions in AKMS .....6-6
6.5.7 (U) Five Digit Outgoing Voucher Number.....6-7
6.5.8 (U) Destruction “Certification Statements”.....6-7
6.5.9 (U) Inadvertent Destruction of COMSEC Material.....6-7
6.5.10 (U) Account Transactions to COR.....6-7

6.6 GENERAL INFORMATION ON AKMS ELECTRONIC KEY DISTRIBUTION AND DESTRUCTION
.....6-7
6.6.1 (U) Electronic Key Distribution.....6-7
6.6.2 (U) Electronic Key Destruction.....6-8

**Chapter/Paragraph..... Page**

6.7 ACCESSIBILITY TO THE LMD/KP ..... 6-8
6.7.1 (U) CIK AND PIN Number Storage.....6-8
6.7.2 (U) LMD/KP "Disaster Recovery Kit" .....6-8
6.7.3 (U) Archiving and Key Processor (KP) Changeover.....6-9
6.7.4 (U) Accountability for KSD-64 Transit CIKS .....6-9
6.7.5 (U) AKMS KP Settings .....6-10
6.7.6 (U) AKMS User Deletion .....6-10

6.8 STORAGE OF LCMS WORKSTATION .....6-11

6.9 ASSOCIATED EQUIPMENT AND REQUIREMENTS .....6-11
6.9.1 (U) STU-III Connectivity .....6-11
6.9.2 (U) Laser Printers .....6-11
6.9.3 (U) DTD .....6-11
6.9.4 (U) Data Cartridge .....6-11

6.10 TRAINING.....6-12
6.10.1 (U) LCMS Operator Training Criteria .....6-12

6.11 LCMS MAINTENANCE ..... 6-12
6.11.1 (U) LMD Accountability.....6-12
6.11.2 (U) Depot Level Repair.....6-12
6.11.3 (U) Replacement KP .....6-12

6.12 ADDITIONAL ARMY PUBLICATIONS ..... 6-12
6.12.1 (U) LMD Software Upgrade .....6-12
6.12.2 (U) Doctrine.....6-13

6.13 COMMUNICATIONS .....6-13

6.14 AKMS ACCOUNT INVENTORIES .....6-13

CHAPTER 7 COMSEC COMPROMISES AND INCIDENTS .....7-1

7.1 COMPROMISES AND INCIDENTS .....7-1

7.2 REPORTING COMSEC INCIDENTS ..... 7-4
7.2.1 (U) Responsibilities .....7-5
7.2.2 (U) Controlling Authority Limitations .....7-6

7.3 COMSEC INCIDENT REPORTS.....7-6
7.3.1 (U) Report Contents.....7-6
7.3.2 (U) Reporting Incidents.....7-6
7.3.3 (U) Report Precedence.....7-6

7.4 ROUTING OF INCIDENT REPORTS ..... 7-7
7.4.1 (U) Incident Reports Involving Joint-Staff Position Control Material.....7-7
7.4.2 (U) Satellites and Space Vehicles .....7-7
7.4.3 (U) Discovery of Listening Devices .....7-9
7.4.4 (U) Compromising Emanations .....7-9

7.5 TRANSMISSION DURING MINIMIZE AND "IN-THE-CLEAR" .....7-9

**Chapter/Paragraph.....Page**

7.6 PHYSICAL INCIDENTS ..... 7-9
7.6.1 (U) Physical Incident Reports .....7-9
7.6.2 (U) Missing Material .....7-10
7.6.3 (U) Temporary Loss .....7-10
7.6.4 (U) Damaged Packages .....7-10
7.6.5 (U) Unauthorized Access.....7-10
7.6.6 (U) Material Left Unprotected.....7-11
7.6.7 (U) Aircraft Crashes .....7-11
7.6.8 (U) Combat Conditions .....7-11
7.6.9 (U) Unauthorized Photography .....7-11
7.6.10 (U) Satellites.....7-11
7.6.11 (U) Controlled Cryptographic Items (CCI) .....7-11

7.7 PERSONNEL INCIDENTS ..... 7-12
7.7.1 (U) Definitions .....7-12
7.7.2 (U) Personnel Incident Reports.....7-12
7.7.3 (U) Captured or Presumed Captured Personnel.....7-12
7.7.4 (U) Personnel Absence .....7-12
7.7.5 (U) Revocation or Suspension of Clearance for Cause.....7-13

7.8 CRYPTOGRAPHIC INCIDENTS .....7-13
7.8.1 (U) Equipment Malfunctions .....7-13
7.8.2 (U) Unauthorized Cryptoperiod Extension.....7-13

7.9 ADMINISTRATIVE INCIDENTS……..7-13

7.10 INVESTIGATIONS .....7-14

7.11 EVALUATIONS .....7-14

7.12 INCIDENT CASE FILES……...7-14

7.13 REVIEWING AND MARKING COMPROMISED MESSAGES..... 7-14
7.13.1 (U) Reviewing Messages.....7-14
7.13.2 (U) Marking Messages .....7-15

7.14 RELIEF FROM ACCOUNTABILITY ..... 7-15
7.14.1 (U) Relief from CMCS Accountability.....7-15
7.14.2 (U) Relief from Property Accountability.....7-15

# APPENDIXES


| Appendix Number | Title | Page |
|---|---|---|
| APPENDIX A | REFERENCE REGULATIONS AND FORMS | A-1 |
| APPENDIX B | ABBREVIATIONS AND TERMS | B-1 |
| APPENDIX C | COMSEC NOMENCLATURE SYSTEMS | C-1 |
| APPENDIX D | LOCALLY REPRODUCIBLE FORMS | D-1 |
| APPENDIX E | COMSEC ACCOUNT REGISTRATION PACKET (CARP) | E-1 |
| APPENDIX F | ARMY STRUCTURE FOR COMSEC SUPPORT COMSEC MATERIAL CONTROL SYSTEM (CMCS) | F-1 |
| APPENDIX G | LOCAL PRE-INSPECTION CHECKLIST | G-1 |


# LIST OF ILLUSTRATIONS


| Figure | Title | Page |
|---|---|---|
| Figure 2-1 | EKMS Architecture | 2-1 |
| Figure 2-2 | COMSEC Material Control System | 2-2 |
| Figure 2-3 | COMSEC Facility Approval Request (CFAR) | 2-10 |
| Figure 3-1 | Request to Establish a Cryptonet | 3-9 |
| Figure 3-2 | Request for Resupply of Key | 3-20 |
| Figure 3-3 | Request for Resupply of Key when Key Usage Changes | 3-21 |
| Figure 3-4 | Request for Redistribution of Key | 3-22 |
| Figure 4-1 | COMSEC Material Voucher Control Register (Outgoing) (DA Form 4669-E) | 4-13 |
| Figure 4-2 | COMSEC Material Voucher Control Register (Local) (DA Form 4669-E) | 4-13 |
| Figure 4-3 | COMSEC Aid Items Register (ALC 1 Material) | 4-16 |
| Figure 4-4 | COMSEC Aid Items Register (ALC 4 Material) | 4-17 |
| Figure 4-5 | COMSEC Equipment Items Register. Example for ALC 1 Equipment Accountable by Serial Number | 4-19 |
| Figure 4-6 | COMSEC Equipment Items Register. Example for ALC 2 Items Accountable by Quantity | 4-20 |
| Figure 4-7 | COMSEC Material Disposition Record (DA Form 5941-E) | 4-25 |
| Figure 4-8 | COMSEC Material Report (SF 153) | 4-30 |
| Figure 4-9 | COMSEC Account – Daily Shift Inventory (DA Form 2653-E) | 4-37 |
| Figure 4-10 | COMSEC Account – Daily Shift Inventory (TPI) (DA Form 2653-E) | 4-38 |
| Figure 4-11 | Preprinted Semiannual Inventory Report (SAIR) C&C Page | 4-41 |
| Figure 4-12 | Sample Completed CCIR COMSEC Aids Item Register (ALC 4) (DA Form 2011-E) | 4-43 |
| Figure 4-13 | Sample of Aids Item Register ALC 4 Local Annual Inventory (DA Form 2011-E) | 4-44 |
| Figure 4-14 | Local Accounting of Reproduced COMSEC Accountable Publication (DA Form 2011-E) | 4-48 |
| Figure 7-1 | Unclassified Example - Physical COMSEC Incident Report | 7-16 |
| Figure 7-2 | Unclassified Example - Personnel COMSEC Incident Report | 7-17 |
| Figure 7-3 | Unclassified Example - CCI Incident Report | 7-18 |

# List of Tables


| Table | Title | Page |
|---|---|---|
| Table 3-1 | Digraph for Systems | 3-12 |
| Table 4-1 | Accounting Forms | 4-3 |
| Table 4-2 | Accounting Reports | 4-4 |
| Table 4-3 | Transfer/Receipt Reports | 4-5 |
| Table 4-4 | Destruction Reports | 4-6 |
| Table 4-5 | Inventory Report (Traditional Accounts) | 4-7 |
| Table 4-6 | Modification of Other Services Voucher Numbers | 4-12 |
| Table 4-7 | COMSEC Material Report (SF 153) | 4-28 |
| Table 6-1 | Inventory Reports (AKMS Accounts) | 6-4 |
| Table 6-2 | Deletion of an AKMS User Account from an LCMS Workstation | 6-10 |
| Table 7-1 | Reportable COMSEC Incidents | 7-2 |
| Table 7-2 | Incident Reporting Addressees | 7-8 |

**THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY**

# CHAPTER 1
# GENERAL

## 1.1 PURPOSE.

**1.1.1 (U) Objective.** This Technical Bulletin (TB) provides Communications Security (COMSEC) information regarding custodianship of accounts, accounting/reporting procedures, safeguarding material supply procedures, and Controlling Authority (CONAUTH) responsibilities in accordance with (IAW) COMSEC policy set forth in Army Regulation (AR) 380-40.

**1.1.2 (U) Scope.** This TB includes the following:

**a. (U) Minimum Safeguards**. Defines minimum safeguards and standard criteria and procedures for protecting COMSEC information.

**b. (U) Special Safeguards**. Defines the special safeguards of the Army COMSEC Material Control System (CMCS) and the Army Key Management System (AKMS). The defined safeguards are achieved by the use of correct procedures for the control of access, storage, distribution, accounting, and destruction of COMSEC material.

**c. (U) Accounting Procedures**. Defines accounting procedures for COMSEC material.

**d. (U) Maintaining COMSEC material.** Defines procedures for requesting, receiving, stocking, and reporting COMSEC key, publications, and equipment.

**e. (U) Incorporation of National INFOSEC Policy.** Incorporates the applicable provisions of the National Security Telecommunications and Information Systems Security Instructions (NSTISSI) promulgated by the National Security Agency (NSA), as implemented by AR 380-40.

**1.1.3 (U) References, Abbreviations and Terms.** See Appendixes.

## 1.2 APPLICABILITY.

(U) This TB shall be used by:

**a. (U) Personnel.** All personnel within the active Army, Army Reserve (USAR), Army National Guard (ARNG), Army Reserve Officers' Training Corps (ROTC), civilian government employees of the Army, and Army contractors who are responsible for COMSEC material activities.

**b. (U) COMSEC Accounts.** The procedures contained in this TB apply to both manual and automated accounts; however, some of the procedures and instructions contained herein apply exclusively to manual records, forms, and files. COMSEC Custodians managing automated accounts will adhere to all instructions contained in Army Key Management System (AKMS) documents. Conflicts between this TB and the aforementioned stated documents, which cannot be reconciled, will be reported to the U.S. Army Communications Electronics Command (CECOM), Communications Security Logistics Activity (CSLA) IAW the instructions contained in paragraph 1.4.

## 1.3 AVAILABILITY OF FORMS.

(U) The following forms (see Appendix D) are authorized for local reproduction:

**a. (U) Department of Army (DA) Form 1999-E, Restricted Area Visitor Register** (Figure D-1). This form is also available at the USAPA website (www.usapa.army.mil).

**b. (U) DA Form 2011-E, COMSEC Aids Items Register** (Figure D-2). This form is also available at the USAPA website (www.usapa.army.mil).

**c. (U) DA Form 2011-1-E, COMSEC Equipment Items Register** (Figure D-3). This form is also available at the USAPA website (www.usapa.army.mil).

**d. (U) DA Form 2653-E, COMSEC Account – Daily Shift Inventory** (Figure D-4). This form is also available at the USAPA website (www.usapa.army.mil).

**e. (U) DA Form 4669-E, COMSEC Material Voucher Control Register** (Figure D-5 Front and Reverse). Side 2 of 3 is to be printed on the reverse side of 2 of 2. This form is also available at the USAPA website (www.usapa.army.mil).

**f. (U) DA Form 5251-E, CONAUTH Key Management Worksheet** (Figure D-6). This form is also available at the USAPA website (www.usapa.army.mil).

**g. (U) DA Form 5941-E, COMSEC Material Disposition Record** (Figure D-7). This form is also available at the USAPA website (www.usapa.army.mil).

**h. (U) EKMS Worksheet, Local Electronic COMSEC Material Disposition Record** (Figure D-8). This is a sample worksheet; however, custodians may design a worksheet that will better fit their needs as long as the pertinent information is included (see Appendix D). Reproduce this form on 8½ x13-inch white paper printed head to foot.

## 1.4 RESOLUTION OF CONFLICTS.

(U) Conflicts, which cannot be reconciled locally, and situations not covered by this TB, will be submitted through command channels for resolution to: Director, U.S. Army Communications-Electronics Command, Communications Security Logistics Activity, ATTN: SELCL-ID-P3, Fort Huachuca, AZ 85613-7041. In addition, requests for deviation waivers from the standard procedures prescribed in this TB will be prepared IAW AR 25-30 and submitted through command channels to CSLA.

## 1.5 ARMY COMSEC WHOLESALE LOGISTICS MANAGEMENT PROGRAM.

**a. (U)** CSLA is the Army Wholesale Logistics Manager for COMSEC equipment and Keying Materiel. CSLA is part of a subordinate activity of the U.S. Army Communications-Electronics Command (CECOM; a Major Subordinate Command [MSC] of the Army Materiel Command [AMC]).

**b. (U)** CSLA operates a National Inventory Control Point and National Maintenance Point (NICP/NMP) for COMSEC centrally accountable materiel, and one of the Primary TIER 1 sites (PT1S) for DoD to administer the Electronic Key Management System (EKMS). In its capacity as a Tri-Service EKMS Manager, CSLA staffing includes representatives from the U.S. Navy and U.S. Air Force.

**c. (U)** CSLA maintains a permanent staff of CSLA Information Security (INFOSEC) Representatives (CIRs) in the Continental United States (CONUS) and outside the Continental United States (OCONUS) in Europe and Korea. Personnel assigned to these offices are available for any COMSEC material or account automation assistance you may need. See Appendix F for Points of Contact.

## 1.6 COMMENTS AND RECOMMENDATIONS.

(U) Users are invited and encouraged to send comments and suggested improvements to this TB in DA Form 2028 format directly to CSLA, ATTN SELCL-ID-P3.

## 1.7 INTRODUCTION OF ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS).

**a. (U)** The NSA developed EKMS for joint-use and compatibility throughout all Department of Defense (DoD) services and the Civil Agencies. EKMS enables COMSEC Custodians to generate electronic key by use of a key processor. This system will drastically reduce the amount of physical key within the CMCS by providing for key generation at the account level and making COMSEC accounting virtually transparent to users.

**b. (U)** Army Key Management System (AKMS) is the Army's implementation of the EKMS. AKMS will provide local real-time electronic key generation, distribution, and management in support of Command, Control, Communications, Computers and Intelligence (C4I) at all Army Command levels. AKMS has been incorporated throughout this TB; however, detailed AKMS information resides in Chapter 6. AKMS will perform the following:

(1) (U) Provide accountability and management of existing and future COMSEC material.

(2) (U) Ensure compatibility and interoperability between Army COMSEC accounts and all other services within DoD.

(3) (U) Replace the current ACCLAIMS IV Automation program and most manual accounts.

**c. (U)** Physical Material. Throughout this TB, reference will be made to "Physical (COMSEC) Material." This term is used as a generic phrase to encompass all "hard copy" key, software, publications, equipment items and hardware.

**d. (U)** Electronic Material. Throughout this TB, references will be made to "Electronic (COMSEC) Material." This term is used as a generic phrase to encompass all locally-, Tier 1-, or Central Facility-generated keying material; FIREFLY and modern key; and imported keying material.

## 1.8 SERVICE AUTHORITY.

(U) The "Service Authority" is a new term and will be used throughout this TB. The Army Service Authorities are listed in Appendix F. The approved definition for a Service Authority is as follows: "The service authority is the command or activity within each military service that oversees Communications Security (COMSEC) operations, policy, procedures and training." In the Army, the Headquarters, Department of the Army (HQDA), Deputy Chief of Staff, and G-2 serve in this capacity. Service authority responsibilities are those functions that the military services have determined cannot be performed by the Tier 1. Service authority roles include cryptographic hardware management and distribution control, including Foreign Military Sales (FMS); approving account establishments; approving authority for Certification Approval Authorities (CAAs); implementing COMSEC Material Control System (CMCS)/Key Management Infrastructure (KMI) policy and procedures; direct operational support; final adjudication authority in determining if reported COMSEC Incidents have resulted in COMSEC Insecurities; ensuring service compliance with COMSEC Access Program requirements; and standing membership on KMI working groups and the Tier 1 Joint Configuration Control Board (JCCB).

**THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY**

# CHAPTER 2

# COMSEC FACILITY, CMCS, ACCOUNTS, AND CUSTODIAN REQUIREMENTS

## 2.1 COMSEC MATERIAL CONTROL SYSTEM (CMCS).

**a. (U)** The CMCS was established to provide accountability for all COMSEC material. CSLA maintains PT1S Fort Huachuca Central Office of Record (COR) within the architecture of the EKMS Tier 1 System, which provides a continuous and exact record of centrally accountable (ALC 1, ALC 2, and ALC 6) COMSEC material. Accountable reporting channels for COMSEC material are shown in Figure 2-1. Local accountability is maintained for all other CMCS-accountable material.

**b. (U)** The following paragraphs describe the procedural tasks that support the CMCS and the Army organizations or activities that perform them. As discussed in the following paragraphs, these CMCS components (Figure 2-2 on following page) form the basis for providing COMSEC support to the WARFIGHTER in COMSEC operations.

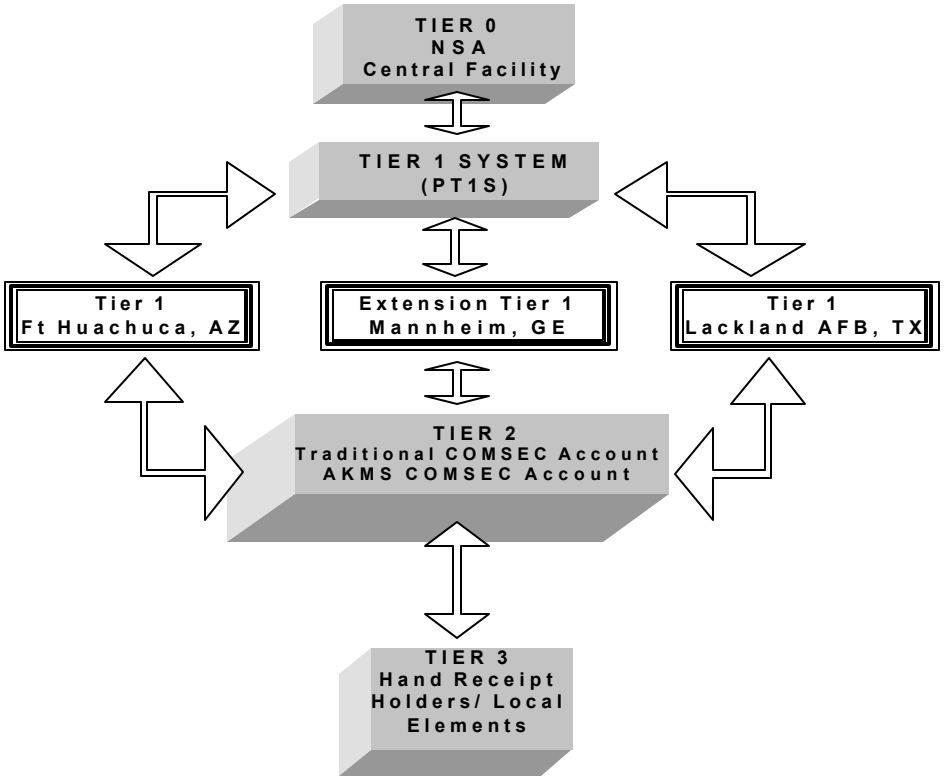



**Figure 2-1. EKMS Architecture**

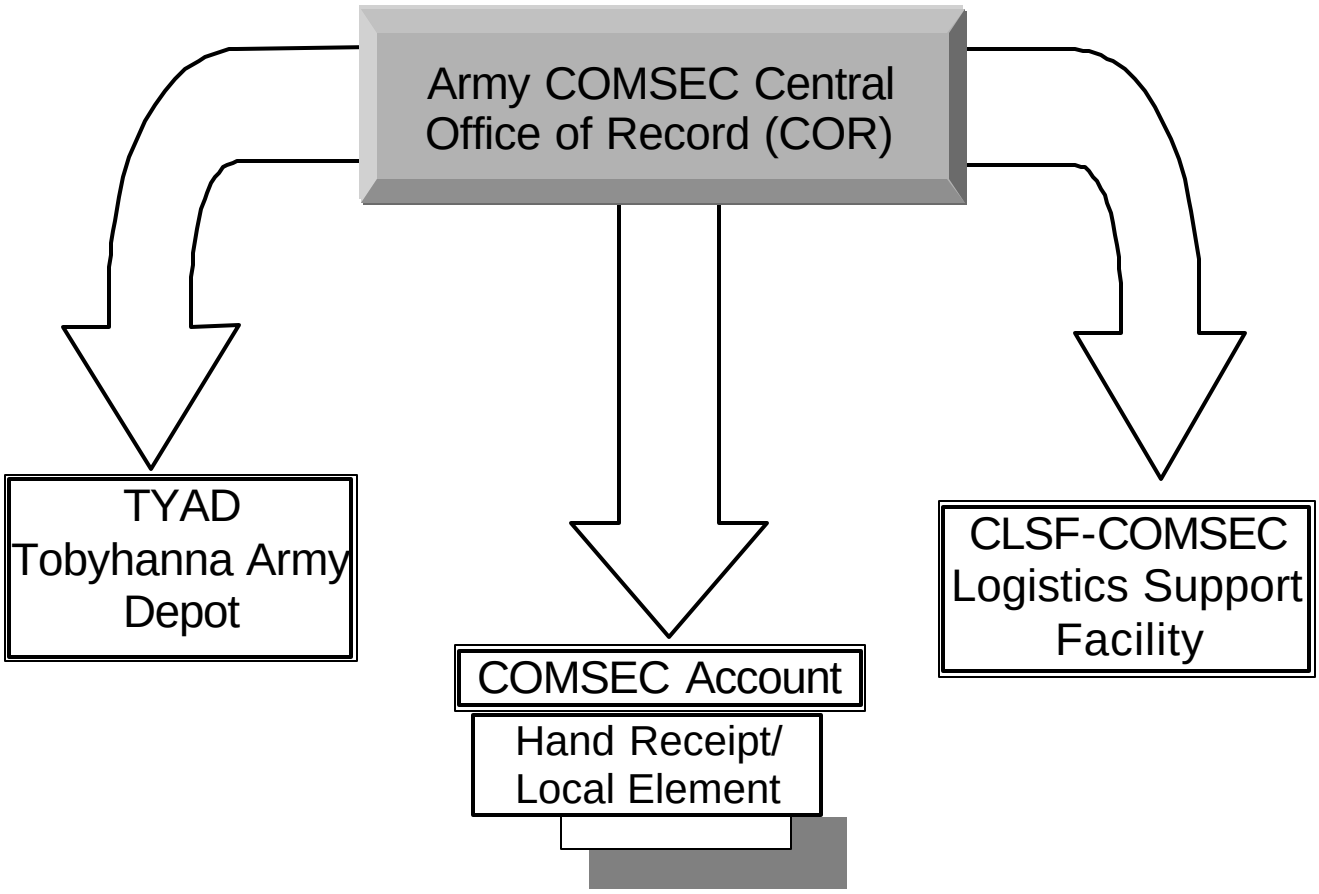



**Figure 2-2. COMSEC Material Control System (CMCS)**

**2.1.1 Army CMCS Structure.**

**a. (U) COR (throughout this TB, the COR may be referred to simply as the Tier 1).** The Tier 1 is a software application that allows it to function as the primary element (component) of the EKMS, which provides critical functions and features at the COMSEC Wholesale Management level required to manage, protect, distribute, and transfer electronic and hard copy key material for Joint-Service COMSEC material.

(1) (U) The Tier 1 is capable of generating and distributing electronic key material for COMSEC equipment.

(2) (U) Under this system, the Tier 1 provides the functions required to maintain the Central Office of Records (COR) for all services.

(3) (U) The Tier 1 performs the account registration, privilege management, ordering, distribution, account, system management, and security management, as well as directs the management and distribution of physical COMSEC material for all services.

(4) (U) The Tier 1 is composed of two major elements and several components that function together to provide a complete and fully operational system for worldwide support of DoD Military Services. The two major elements are the Primary Tier 1 located at Fort Huachuca, Arizona, and administered by CSLA (formerly known as the ACCOR); and the Primary Tier 1 located at Lackland Air Force Base at San Antonio, Texas, and administered by the United States Air Force (USAF). In addition, an Extension Tier 1 (ET1) is located at Mannheim, Germany, to provide in-country support to all service elements in the European Theater of Operations. An additional ET1 may be added in the future to support the Pacific Theater. Some of the specific functions performed by the Primary Tier 1 are as follows:

(a) (U) Maintains records of:

(1) (U) All services' COMSEC accounts by account number.

(2) (U) Master inventories for all accountable COMSEC material.

(3) (U) Correspondence between Tier 1 and COMSEC accounts.

(b) (U) Directs periodic inventories and performs verifications of COMSEC material held by accounts.

(c) (U) Issues Certifications to COMSEC accounts for:

(1) (U) Verification of satisfactorily conducted and properly reported inventory.

(2) (U) Clearance and relief from accountability for former COMSEC Custodian(s).

(d) (U) Removes from CMCS accounting any COMSEC material that has been lost, stolen, or destroyed without proper certification or authorization as directed by the Service Authority for Army Incidents.

(e) (U) Provides central accountability for all centrally accountable COMSEC material to include positive-control material.

(f) (U) Serves as the Registration Authority for all accounts.

(g) (U) Executes key ordering/ generation for traditional and modern key.

(h) (U) Maintains a current COMSEC Account Registration Packet (CARP) for each Army account at its supporting Tier 1 site.

(i) (U) Issues Privilege Certificates to all Tier 2 users.

**b. (U) Extension Tier 1 (ET1).** An ET1 serves as a communications connector to the Tier 1. When directed, or during contingencies, an ET1 can function as registration authority and an ordering authority for the COMSEC accounts it supports. ET1 will not function as a COR except when directed in wartime or during other emergencies. ET1 maintains a defined distribution formula to support customers: it may order key material from the TIER 1 or direct appropriate local generation of key material to satisfy theater requirements. This requires an ET1 to maintain the capability for key material generation, translation, packaging and distribution. In addition, an ET1 has the functional capabilities to maintain local accounting records for COMSEC material (i.e., hard copy and electronic key material as well as centrally accountable COMSEC equipment), provide accounting functions, and respond to queries regarding account management. ET1 supports the enforcement of ordering, distribution, generation, and short title assignment privileges at the COMSEC accounts within its area of responsibility.

**c. (U) COMSEC Accounts (Tier 2).** COMSEC accounts managing key and other COMSEC material by use of the AKMS are also referred to as Tier 2. All COMSEC accounts will be considered as either a Local or a Peer COMSEC Account. A Local COMSEC Account is the COMSEC account that initiates action. A Peer COMSEC Account is the account that receives the action from the Local COMSEC Account. Neither the COR nor the Central Facility (CF) are considered Local or Peer COMSEC Accounts. Those included in this category consist of:

- (U) Traditional Accounts. COMSEC accounts conducting accounting functions manually; and,

- (U) AKMS Accounts. COMSEC accounts conducting accounting and key generation functions using the LCMS Workstation.

(1) (U) COMSEC Wholesale Depot. The COMSEC Directorate at Tobyhanna Army Depot (TYAD) has been designated to store and issue all COMSEC material centrally managed as wholesale stocks by CSLA. It also provides depot-level maintenance support for COMSEC equipment in the Army inventory, worldwide. All depot functions for equipment are performed by TYAD. The U.S. National Distribution Authority (USNDA) administered by the National Security Agency (NSA), with its distribution point located at Hanover, MD, exclusively performs wholesale-level physical key material storage and distribution.

(2) (U) COMSEC Logistics Support Facility (CLSF). A CLSF is any designated support element in the Army that provides retail- or wholesale-level COMSEC material distribution, supply, storage or maintenance service to a field Army or equivalent force, Corps, or Division.

(3) (U) Maintenance Activities. COMSEC accounts designated by the Major Army Commands (MACOMs) and approved by HQDA to perform specific COMSEC equipment maintenance functions.

(4) (U) Operational Accounts. Active units that are authorized accounts, and who require COMSEC material in the performance of their missions. These accounts are normally established below Division level.

(5) (U) RDT&E Accounts. COMSEC accounts designated for Research, Development, Testing and Evaluation.

**d. (U) COMSEC Hand Receipt Holder (Tier 3)**. This COMSEC Hand Receipt Holder level, also referred to as Tier 3, is the level of COMSEC operations where Hand Receipt Holders and users of COMSEC equipment and key receive direct support from the Tier 2 COMSEC Custodian. The COMSEC Custodian should inspect Hand Receipt Holders once a year. When it is not possible for the custodian to personally inspect each Hand Receipt Holder due to widespread and distant dispersion, the custodian will require each Hand Receipt Holder to complete a self-inspection and inventory prepared by the custodian. The Hand Receipt Holder must certify inventory accuracy of his/her holdings as well as compliance with all security, control and accounting requirements mandated by AR 380-40 and this TB. The COMSEC Custodian will maintain, on file, a record of the

inspection/inventory for review by Command Inspectors and CSLA Auditors. COMSEC accounts will hand receipt to individuals. Hand Receipt Holders are required to:

(1) (U) Sign for accountable COMSEC material received.

(2) (U) Safeguard COMSEC material in their possession and provide secure storage as prescribed in AR 380-40.

(3) (U) Promptly report COMSEC Incidents, as directed.

(4) (U) Comply with local accounting procedures for assigned COMSEC material, as directed by the custodian.

(5) (U) Conduct daily shift-to-shift inventories, as specified in paragraph 4.12.

**e. (U) EKMS ID.** Within the EKMS architecture, EKMS ID Numbers are required to identify COMSEC accounts, establish credentials, and execute transactions between the various elements and activities operating throughout the system. A separate EKMS ID will be assigned to individuals or activities as follows:

- (U) Tier 2 COMSEC Accounts
- (U) Central Office of Record
- (U) Tier 1 Registration Authority
- (U) Controlling Authorities (who do not manage an EKMS COMSEC Account)
- (U) User Representative
- (U) Command Authority

At the Tier 2 level, with the exception of a few existing Army COMSEC accounts, the EKMS ID will be the established COMSEC Account Number.

**2.1.2 (U) CMCS Addresses.** The CMCS uses six different types of addresses:

**a. (U) Mailing Address** (the physical address for receiving mail). This address will include the COMSEC Account Number in the attention (ATTN) line. For example:

Commander
HHD 41ST Signal Battalion
Unit 15258
ATTN: COMSEC Account 5A0299
APO AP 96205-0031

**b. (U) Physical Location**. This address is the physical location of the account. The physical location will consist of Unit designation; ATTN: COMSEC Account (number); physical location (e.g., street address, building number, Kaserne name, room number); and city, state or country. For example:

Commander
1ST Signal Brigade
ATTN: COMSEC Account 5A2099
CLSC-K-Maintenance Division
Building S-1096, Room 22
Camp Coiner, Seoul, Korea

**c. (U) Defense Message Service (DMS) Address.** DMS addresses can be found in your DMS directory.

/C=US/O=U.S. Government/OU=DoD/OU=ARMY/OU=Organizations/L=CONUS/L=FORT HUACHUCA AZ/OU=CSLA/OU=CSLA Incidentdesk 1(uc)

**d. AUTODIN Message Address.** This addressing system, which is being phased-out in favor of the DMS system, is composed as directed in DA Pam 25-100-1.

CDR CLSCKMTDIV1STSIGBDE
SEOUL KOR //5A0299//

**e. (U) Defense Courier Service (DCS) Address.**

(1) (U) This address is used for the delivery of material shipped via DCS. The address consists of two lines and is placed on the exterior wrapper of the package. The first line contains the COMSEC Account Number, a dash, a two-letter Defense Courier Service Station digraph, and a two-number routing suffix. The second line contains the unit's abbreviated title (without designations such as HHC, HQ, etc.). For example:

5DR300RA20
918th SIG CO DET A

(2) (U) Deliveries of COMSEC material sent through DCS will be made to the COMSEC account DCS station; not the COMSEC account physical address. It is the responsibility of the custodian to pick up, or ensure the pick up by authorized personnel, the shipment at the DCS station or from a DCS courier.

(3) (U) When establishing a new account or a CHANGE to an account, the custodian must provide the DCS station a copy of the new CARP and 3 copies of DCS Form 10.

(4) (U) DCS addresses will be provided to the COMSEC account by the DCS station after submission of required documentation. Refer to DCS 5200.1-M for instructions on filling out the form. (This publication is not available through publication channels; it must be obtained directly from DCS.)

(5) (U) Notify CSLA upon receipt of the DCS address. Provide CSLA with the DCS routing code assigned to the account.

**e. (U) Internet Protocol (IP) Address.** This address is for accounts reporting to Tier 1 via an LCMS Workstation. The IP Address is assigned by CSLA and allows access to the Tier 1 message servers.

**2.1.3 (U) COMSEC Directory Service (formerly COMSEC Account Address Directory).** The Registration Authority at the COR maintains the COMSEC Directory Service. The Directory Service lists all COMSEC accounts and contains each account's mailing, message, DCS address and physical location. AKMS accounts can access this information via their LCMS Workstation. Traditional COMSEC accounts must contact the COR for access to account information.

## 2.2 COMSEC FACILITY.

**2.2.1 (U) Approving Office for the COMSEC Facility.** Headquarters, Department of the Army (HQDA) has delegated COMSEC Facility Approval Authority to CSLA. All requests for COMSEC Facility Approvals must be addressed to CSLA.

**2.2.2 (U) COMSEC Facility Approvals.** Each organization or activity that has determined the need for a COMSEC account requires a COMSEC Facility Approval (CFA) from CSLA. Approval will be obtained prior to establishing, performing major alterations that affect physical security, relocating, or upgrading the classification of a COMSEC Facility. Requests for a CFA will be submitted by the local commander through normal command channels to CSLA, based on established Major Command (MACOM) or Major Subordinate Command (MSC) policies. An updated CFA need not be routed through your chain of command unless dictated by local command policies.

**a. (U) Change of Security Level**. When a traditional account or AKMS account requires any security level change, a new COMSEC Facility Approval Request (CFAR) must be submitted. However, an LCMS account requires a new COMSEC Account Number, a new KOK-22A, all new FIREFLY and associated KOK-22A keys, and the transfer of all materials from the existing account to the new account. Additionally, when an AKMS account must change its security classification level, it must contact the CSLA Help Desk for detailed instructions. See Figure 2-3 for a sample CFAR.

**b. (U) Additional Equipment Received.** A new/updated CFA is not required when a new equipment system or new software is brought into an account unless the facility must be upgraded to accommodate the system.

**c. (U) COMSEC Facility Approval for Hand Receipt Holders**. The need for a COMSEC Facility for a Hand Receipt Holder will be determined by the COMSEC account custodian based on unique circumstances or mission requirements, such as large volumes of required material. If the COMSEC account custodian determines that the Hand Receipt Holder will be required to have a COMSEC Facility Approval, the COMSEC account custodian will approve the facility by use of a memorandum, which will include the information listed in paragraph 2.2.3. The memorandum will be retained, on file, in the COMSEC account files for review by COMSEC Inspectors and Auditors.

**d. (U) Duration of COMSEC Facility Approval**. The CFA is valid as long as the physical protective measures and security procedures, which were the basis for the approval, remain substantially unchanged. (See AR 380-40 for additional information.)

**2.2.3 (U) Request for Approval.** The request memorandum will be prepared using the general guidelines contained in the following paragraph. When establishing an account, attach a signed copy of the CARP. A separate request will be submitted for each COMSEC Facility approval being requested. As a minimum, the memorandum will be marked "FOR OFFICIAL USE ONLY" (FOUO). The following information will be provided on each CFAR submitted to CSLA (see Figure 2-3).

**a. (U) General Information.**

(1) (U) Requesting organization's complete mailing address.

(2) (U) Unit Identification Code (UIC).

(3) (U) Telephone number (DSN and commercial).

(4) (U) COMSEC account number (if assigned; otherwise, leave blank).

(5) (U) Location of the facility (includes building, floor and room numbers).

(6) (U) Point of contact (name and telephone number).

(7) (U) Type of request (initial request or modification).

(8) (U) Classification information (the highest level/classification of material that will be used and/or stored)

**b. (U) Purpose**. Indicate the primary purpose of the facility:

(1) (U) *Operations* (on-line or off-line crypto-operations using cryptosystems).

(2) (U) *Distribution* (primary mission is COMSEC logistics support).

(3) (U) *Maintenance.*

(4) (U) *RDT&E* (Research- Development-Testing and Evaluation).

(5) (U) *Other* (if your account does not fall into one of the previous categories, explain its purpose).

**c. (U) Physical Security.** The planned physical security measures must be described in detail. Physical security description of the facility will indicate overall construction composition, to include walls, ceiling, floors, windows, doors, access control, and other measures designed to prevent overt or covert access. If TOP SECRET (TS) material will be stored, include planned provisions to secure TS material IAW Two Person Integrity (TPI). For example, an OCONUS account would include the use of a Joint-Service Interior Intrusion Detection System (J-SIIDS). Also provide the General Services Administration (GSA) description of all security containers used within the facility.

**d. (U) Material and Equipment Security.** Describe, in detail, how classified COMSEC material and equipment will be protected during non-working hours, or when not under the direct and continuous control of properly cleared and authorized personnel; that is, stored in approved containers, vaults, strong rooms, and so forth.

**e. (U) Standards Statement**. Prepare a statement, which certifies that applicable standards for the operation, storage, and destruction of COMSEC material can be met. These standards are as described in Chapters 4 and 5. Organizations, which have standard Positive Control Material (PCM) and/or Two Person Integrity (TPI) material, will include ONLY that information which applies to the standard material (for PCM refer to CJCSI 3260.01).

**f. (U) The CFAR will also contain a statement** that the commander has evaluated the risks to the facility and found them acceptable (AR 380-40, paragraph 4-2b).

**2.2.4 (U) Action by Approving Authority.** CSLA will promptly notify the requesting commander when the CFAR is approved. If the CFAR is not approved, CSLA will inform the commander what action is necessary to obtain approval.

## 2.3 ESTABLISHING A COMSEC ACCOUNT.

**a. (U) Requirement.** The decision to establish a COMSEC account or other type of EKMS ID is a commander's prerogative based on operational necessity. Whenever feasible, COMSEC support should be requested from and provided on a geographical basis using COMSEC accounts which are already established.

**b. (U) Number of Accounts.** The number of established COMSEC accounts will be kept to a minimum consistent with support and security considerations. Providing local commanders concur, there is no objection to COMSEC accounts crossing command lines. This practice is encouraged when it results in economy of resources. However, the local commanders must consider their respective unit missions and whether COMSEC accounting support can be sustained under all contingencies (e.g., mobilization, deployment, tactical operations). The commitments of both units should be documented in a Memorandum of Understanding or Agreement (MOU/MOA) or other formal support agreement.

**c. (U) Establishing a COMSEC Facility**. To establish a new COMSEC account, the unit must submit a signed COMSEC Account Registration Packet (CARP) (formerly DA Form 2012) and a copy of the COMSEC Facility Approval Request (CFAR) to CSLA. To establish a Contractor account, the custodian must also provide a DD Form 254 (Department of Defense Contract Security Classification Specification Form). CSLA will provide the CFAR and the CARP to the COR for account number establishment.

## 2.4 COMSEC ACCOUNT NUMBERING SYSTEM.

**a. (U) COMSEC Account Number.** Each COMSEC account established is assigned a unique six-position account number by the COR.

**b. (U) Closed COMSEC Account Number.** COMSEC Account Numbers assigned to accounts that have closed will not be reassigned to another COMSEC account for at least two years.

**c. (U) AKMS COMSEC Account Numbers. The** COMSEC Account Registration Package (CARP) must be submitted to CSLA. An EKMS ID (Account Number) will be assigned by the COR.

**d. (U) Change of COMSEC Account Number.** With the implementation of the Army Key Management System (AKMS), the only significant digit in the COMSEC Account Number will be the first digit, signifying service or agency. Therefore, there will no longer be a need to change account numbers.

**2.4.1 (U) COMSEC Account Number/EKMS ID Structure.**

**a. (U) First Position.** Indicates the service or agency. Examples are as follows:

(1) (U) Navy, Marine Corps, Coast Guard, Military Sea Lift Command – 0-3

(2) (U) DCS – 4

(3) (U) Army – 5

(4) (U) Air Force – 6

(5) (U) NSA – 8

**b. (U) Second – Sixth Position.** Randomly assigned alphanumeric characters.

**2.4.2 (U) Hand Receipt Numbers (Local Element).** AKMS accounts will register their Hand Receipt Holders as "Local Elements." AKMS accounts will manage all transactions that are directed to the Local Element. AKMS accounts must refer to the Local Management Device/Key Processor (LMD/KP) Operators Manual for further information on Local Elements.

## 2.5 COMSEC ACCOUNT REGISTRATION PACKET (CARP).

**(U) The CARP is a multi-purpose form:** it serves as Appointment Orders for the COMSEC Custodian, as a Request for Establishment of a COMSEC Account, and to report changes. It is

used to record all necessary data that applies to a particular account. A copy of the COMSEC Facility Approval (CFA) or a completed COMSEC Facility Approval Request (CFAR) must be submitted with the CARP when establishing a new account. The required format for the CARP is shown in Appendix D and may be reproduced.

**a. (U) Establishment of a COMSEC Account or EKMS-ID**. To request the establishment of a COMSEC account or EKMS ID, see paragraph 2.3. A copy of the CFAR must be sent with the CARP when establishing a new account.

**b. (U) Appointment of a New COMSEC Custodian or Alternate Custodian**. Provide information on the COMSEC Custodian and alternate custodian(s) appointed IAW the criteria shown in paragraph 2.3.

**c. (U) Report Changes.** Report changes to any of the information required on the CARP IAW paragraph 2.5.3, which enables Tier 1 to ensure the Directory CAAD is maintained with current information.

**2.5.1 (U) COMSEC Account Registration Packet (CARP) Distribution.**

**a. (U) Distribution**. The COMSEC Custodian will submit one copy of the CARP to CSLA by mail or fax, and one copy will be retained for the local file.

**b. (U) Expedited Establishment or Change**. When a COMSEC account is established or changed on an expedited basis, a CARP may be submitted to CSLA by electronic transmission. Following electronic transmission of the CARP, a signed copy will be forwarded to CSLA by regular mail or fax.

**2.5.2 (U) Reporting COMSEC Account Data Changes.** A modified CARP must be submitted to the COR upon completion of a Change of Custodian Inventory Report (CCIR) and when any information on the memorandum changes except for the number of Hand Receipt Holders. Changes to Hand Receipt Holders will only be reported when a modified CARP is submitted for another reason. When a modified CARP is submitted as a change, all of the paragraphs, including the paragraphs that have not changed, must be completed. The custodian must also notify the CONAUTH of any unit identification or address changes.

**2.5.3 (U) Completion of the CARP.** The CARP will be completed using the sample in Appendix E of this TB.

**2.5.4 (U) Fund Code Department of Defense Activity Address Code (DODAAC).** The Standard Financial System (STANFINS) requires a DODAAC to identify the appropriate Finance and Accounting Office (F&AO) to which billings will be sent. The CARP specifically requires the COMSEC Account DODAAC. This will be used by CSLA to determine the customer's servicing F&AO. Therefore, it is imperative that COMSEC Custodians periodically review the DOD Activity Address Directory (DODAAD) to verify that assigned unit/account DODAACs are valid. If the DODAAC recorded on the CARP is incorrect, immediately submit a modified CARP to CSLA.

## SAMPLE OF COMSEC FACILITY APPROVAL REQUEST (CFAR)

DEPARTMENT OF THE ARMY
*HEADQUARTERS, YOUR UNIT DESIGNATOR*
*MAILING ADDRESS*

***YOUR OFFICE SYMBOL*** (380-40A)

MEMORANDUM THRU COMMANDER, YOUR HIGHER HEADQUARTERS, MAILING ADDRESS

FOR DIRECTOR, UNITED STATES ARMY COMMUNICATIONS SECURITY LOGISTICS ACTIVITY, ATTN: SELCL-ID-SAS, FORT HUACHUCA, AZ 85613-7041

SUBJECT: COMSEC Facility Approval Request (CFAR)

1. Reference
   a. AR 380-40, Chapter 4
   b. TB 380-41, Chapter 2

2. This command has a requirement to ***establish*** or ***update*** (complete as appropriate) a COMSEC Facility.

   a. General Information
   (1) Requesting Unit: Unit ***Designation, Mailing Address***
   (2) UIC: ***Wxxxxx***
   (3) Telephone Numbers: Commercial ***and DSN*** (OCONUS: Use Full commercial telephone number to include country code.)
   (4) COMSEC Account Number***: 5xxxxx*** (Leave blank if for establishment of a COMSEC account, the number will be determined by your TIER 1 Central Office of Record
   (5) Facility Location: ***Actual location, floor, room, building number, to include street.*** If requesting a security container as your facility, state: ***GSA Approved Security Container within room xxx***
   (6) Point of Contact: Name, ***e-mail address and complete telephone number if different from above***
   (7) Type of Request: Initial (establishment), ***Relocation, Update, etc.***
   (8) Classification information: Highest ***classification of material received or held***

   b. Purpose: ***Operations, Distribution, Maintenance, RDT&E, Other IAW TB 380-41, Chapter 2.*** (Indicate your Primary Purpose!)

   c. Physical Security: ***Provide physical security description of the facility, IAW TB 380-41, Chapter 2 and AR 380-40. Also, identify any type of Alarm system. If the request is for a TS facility, identify the provisions to store the material, IAW TPI. If the facility is to be a GSA approved security container, identify SECONDARY BARRIERS; include ACCESS control when the container is open.*** (Example: Room ___ is constructed of 8" block on the outside wall and sheet rock on the inside walls. All walls go from true floor to true ceiling. There is one window in the room on the outside wall that can be locked from the inside, which has drapes to prevent unauthorized viewing. The only entry into the room is through a hollow core door, which has inside hinges and is secured with a key lock. There is an air conditioner protruding through the outside wall. The AC unit cannot be removed from the outside. TS material will be stored in a GSA approved security container having dual combination locks.)

   d. Material and Equipment Security: ***Describe protection of material during nonworking hours, IAW TB 380-41, Chapter 2*** (Example: All classified COMSEC material will be stored in GSA approved security containers and the door to the COMSEC Facility will remain locked during non-working hours.

3. Standards Statement: ***Prepare a statement certifying whether the applicable standards can or cannot be met, IAW TB 380-41, Chapter 2***. (Example: The standards for the operation, storage and destruction of COMSEC materials as set forth in TB 380-41 can be met).

4. The Commander has evaluated the risks to the facility and found them to be acceptable.

**SIGNATURE BLOCK OF COMMANDER**

(Signed by the Commander)

**CLASSIFICATION AS APPROPRIATE**

## Figure 2-3 COMSEC Facility Approval Request (CFAR)

## 2.6 SUPERVISION OF COMSEC FACILITIES.

(U) In discharging their responsibilities, each commander will make sure the following requirements are satisfied:

**a. (U) Policy and Procedures.**

(1) (U) All accounts must have a reference file containing a copy of AR 380-40, TB 380-41, AR 710-2, DA PAM 25-380-2, and a copy of the local Emergency Plans (where required).

(2) (U) A COMSEC SOP is highly recommended; however, AR 380-40 does not require it.

**b. (U) Personnel Training.** The commander must ensure that each individual is fully qualified to perform the appointed duties as a COMSEC Custodian or alternate.

(1) (U) Custodians must meet the requirements of paragraph 2.7.

(2) (U) COMSEC account custodians will ensure Hand Receipt Holders and users are properly trained to use, protect, and safeguard COMSEC material.

(3) (U) Certification of maintenance personnel will be reflected on DD Form 1435 (COMSEC Maintenance Training and Experience Record) as prescribed by AR 25-12.

**c. (U) Reporting.** All reports required in this TB must be submitted promptly and accurately.

**d. (U) Physical Security.** Continuous physical security within the COMSEC Facility must be maintained to preclude access by unauthorized individuals.

**e. (U) Emergency Plans.** See Chapter 5, paragraph 5.17.

## 2.7 COMSEC CUSTODIAN AND ALTERNATE REQUIREMENTS.

**2.7.1 (U) Custodian and Alternate Appointments.** Concurrent with the establishment of a COMSEC account, the commander will appoint a COMSEC Custodian and at least one alternate. For accounts that hold Positive Control Material (PCM), a minimum of four alternates is required. For accounts that hold TOP SECRET material, three alternates are required. The CARP will be used for the appointment of a COMSEC Custodian and alternate(s). In the appointment of a custodian and alternate(s), the following criteria will apply:

**a. (U) Access Requirements.** Individuals appointed as a COMSEC Custodian or alternate must meet all requirements as directed by AR 380-40. **As a reminder to the commander**, "The security clearance of the COMSEC Custodian and alternates must be, <u>as a minimum,</u> equivalent to the highest classification of material required. IAW AR 380-67, Personnel Security, an "interim clearance" is authorized for COMSEC Custodians and alternates. *Personnel in accounts holding NATO material may be required to have a "final" security clearance to perform custodian or alternate duties*.

**b. (U) Rank or Grade.** The COMSEC Custodian will be a commissioned officer or warrant officer, whenever possible. If a commissioned or warrant officer is not available, a carefully selected noncommissioned officer or a permanent DA civilian (**not** a government contractor) meeting the following grade, rank, or equivalent pay criteria may be appointed:

(1) (U) The enlisted and civilian minimum grade limitations are Staff Sergeant (pay grade E6/GS-7) for COMSEC Custodians, and a minimum of Sergeant (pay grade E5/GS-5) for alternates. IAW AR 380-40, the MACOM commander is authorized to grant waivers to a Sergeant (pay grade E5/GS-5) as a custodian, or Corporal (pay grade E4/GS-4) as an alternate. A copy of the waiver will be kept on file with the CARP in the COMSEC account.

(2) (U) Wage grade personnel may be appointed as custodians provided they are of the salary equivalent to those required for GS employees.

(3) (U) U.S. commercial contractors should refer to DODD 5220.22-R, DODD 5220.22-M, and DODD 5220.22-S. A contractor will **not** be appointed as the custodian of an active Army account.

(4) (U) Under extraordinary circumstances, a commander may appoint U.S. citizen government contractor personnel as "Alternate" COMSEC Custodians. These individuals must meet all training and access security requirements mandated for U.S. Government employees.

**c. (U) Training**. With the implementation of AKMS, there are two different requirements for training depending on the type of account:

· **(U) Traditional Accounts**: The appointed COMSEC Custodian must have successfully completed the Standardized COMSEC Custodian Course (SCCC). When a graduate of the SCCC is not available, the commander may temporarily appoint an untrained COMSEC Custodian; however, the COMSEC Custodian must successfully complete this course within six months after their effective date of appointment. (Any person appointed as a COMSEC Custodian prior to 1 January 1988 and who is and has continuously been a COMSEC Custodian shall be considered "grandfathered" and is not required to attend the SCCC. The "grandfathered" COMSEC Custodian will not be cited for a deficiency or shortcoming during any audit or inspection for not successfully completing the SCCC.)

· **(U) AKMS Accounts**: The appointed COMSEC Custodian must have successfully completed the SCCC, *and* two individuals from each account (usually the COMSEC Custodian and one alternate custodian) must complete formal Local COMSEC Management Software (LCMS) training. Unlike a traditional account, the COMSEC Custodian and alternate must be trained *prior* to assuming the responsibilities of an AKMS account.

- **(U) Alternate Custodian Training:** It is highly recommended that alternate custodians receive SCCC training. Should an alternate custodian fail the SCCC, they may still assume responsibilities of an alternate custodian, but under no circumstances will be appointed as the COMSEC Custodian.

- **(U) Verification of Training:** All exceptions to training requirements must be approved by HQDA, DCS, G-2. In addition, when a MACOM has approved a custodian to be appointed who has not successfully completed the SCCC, the approval must be provided to CSLA, COR. Without written documentation that either HQDA or the accounts MACOM has provided, CSLA will not be able to process the assignment of the custodian or alternate. (See AR 380-40, paragraph 2-2.)

**d. (U) Custodial Obligations.** *Attention Commanders:* An individual will **not** be appointed custodian if other assigned duties do not allow sufficient time for conducting their custodial responsibilities. An extensive list of duties the custodian, alternate, and witness must perform in doing their respective jobs are identified in paragraph 2.7.2. Depending on the size of the account's workload, these duties can easily amount to a full time job and must be taken into consideration in assigning additional duties for these individuals. Prior to appointment as custodian, it must be determined that the individual has at least 12 months (9 months for short tour locations) of service retainability prior to Permanent Change of Station (PCS) or separation. At no time will any individual be appointed as a COMSEC Custodian or Alternate COMSEC Custodian over more than one Army COMSEC account.

**2.7.2 (U) Custodian/Alternate and Witness Duties.**

**a. (U) COMSEC Custodian.** The custodian's duties involve actions pertaining to accountable, COMSEC material charged to the account. The custodian must be thoroughly familiar with the procedures for handling COMSEC material. In larger activities where the size of the COMSEC account prevents the custodian from personally performing required actions and duties, these actions and duties may



FOR OFFICIAL USE ONLY

be performed by other designated and appropriately cleared personnel under the direct supervision of the custodian. Duties of the COMSEC Custodian are as follows:

(1) (U) Establish and maintain accurate accounting records and files. Instructions for file numbering, retention, and disposition of COMSEC files can be found in AR 380-40, Appendix C and in Chapter 4 of this TB.

(2) (U) Keep informed on COMSEC matters pertaining to the customers serviced by the COMSEC account (e.g., Hand Receipt Holders).

(3) (U) Receive, store, transfer and maintain accountability for all COMSEC material issued to the COMSEC account.

(4) (U) Maintain records and prepare reports for accountable COMSEC material.

(5) (U) Maintain a current inventory of all COMSEC material and be aware of the location of such material and the purpose for which it is held. A Semiannual Inventory Report (SAIR) will be completed every six months (for AKMS instructions, see paragraph 6.4.1).

(6) (U) Conduct, supervise or cause required inventories to be performed, including daily or shift-to-shift inventories.

(7) (U) Ensure COMSEC publications are authorized and current per DA PAM 25-35, and that all amendments are properly and promptly entered. COMSEC Logistics Support Facilities (CLSF) and Physical Material Handling Segments (PMHS) are exempt from posting amendments for material that is held in stock for further distribution.

(8) (U) Destroy COMSEC material as prescribed or directed.

(9) (U) IAW Controlling Authority (CONAUTH) direction, requisition COMSEC material for issue to properly cleared individuals whose duties require the material. The custodian will advise each individual of their responsibilities for safeguarding material while in their possession.

(10) (U) Report any compromise or COMSEC Incident of COMSEC material, as directed in Chapter 7.

(11) (U) Maintain stockage levels for operational and contingency key, as shown in Chapter 3.

**b. (U) Alternate COMSEC Custodian.**

(1) (U) The routine duties of the alternate custodian are determined by the custodian and may include any or all of the duties prescribed for the custodian.

(2) (U) The Alternate COMSEC Custodian shall continue to manage the operation of the COMSEC account in the absence of the COMSEC Custodian.

**c. (U) COMSEC Witness.** A witness must authenticate all Semiannual Inventories and destruction of COMSEC material. Any U.S. Government employee (military or civilian) selected to witness a physical inventory or destruction of COMSEC material must have a security clearance equal to or higher than the classification of the material being inventoried or destroyed. It is imperative that the witness:

(1) (U) Be aware that a witness is equally responsible for the accuracy of reports, inventories and physical destruction of the material.

(2) (U) Be aware that a witness can be held accountable under U.S. Civil Codes and the Uniform Code of Military Justice for improper performance of this official duty.

(3) (U) Be physically present and view the action of the custodian when inventorying or destroying COMSEC material.

(4) (U) Sign the report certifying that the COMSEC material listed on the report has been inventoried or destroyed by the COMSEC Custodian, Alternate COMSEC Custodian, or Hand Receipt Holder.

## 2.8 COMSEC CUSTODIAN ABSENCE.

(U) Under no circumstances will the custodian and alternate custodian be absent at the same time. Where possible, it is highly recommended that commanders appoint two or more alternate custodians to prevent concurrent absences.

**a. (U) Temporary Absence (not to exceed 60 days)**. For temporary absences not exceeding 60 consecutive days, the alternate custodian will assume all responsibilities and duties of the custodian. IAW AR 380-67, Personnel Security, a COMSEC Custodian or alternate who possess an "interim clearance" is authorized to perform these duties. Upon return from any prolonged absence, the custodian will perform the following actions:

(1) (U) Review all changes and transactions that took place during the custodian's absence.

(2) (U) If during the absence of the COMSEC Custodian, the alternate custodian receipted for accountable COMSEC material, the COMSEC Custodian will inventory the received material immediately upon his/her return. The custodian will sign and date the COMSEC accounts copy of the Transfer Report. Below the "NOTHING FOLLOWS" entry on the report, the custodian's signature shall be accompanied by the remark "Received from the alternate." This relieves the alternate custodian of responsibility for the received COMSEC material. For AKMS accounts, the alternate will print a copy of the transaction and provide it to the custodian upon his/her return to ensure that the custodian can identify all receipts generated during his/her absence.

(3) (U) If a scheduled or special inventory was performed by the alternate during the custodian's absence, the custodian will verify, sign, and date the file copy of the report and enter the remark "Verified by COMSEC Custodian" below the "NOTHING FOLLOWS" entry.

**b. (U) Extended Absence (exceeding 60 days).** When a COMSEC Custodian is scheduled to be absent from the account for extended periods, the commander must consider and evaluate the impact of such an absence with regard to mission accomplishment and accountability of COMSEC material. For absences exceeding 60 consecutive days, the commander will direct the transfer of the account to the alternate custodian or other individual meeting the requirements of paragraph 2.7.1.b. This will be accomplished by submitting a modified CARP and a Change of Custodian Inventory Report to the COR.

**c. (U) Sudden Unscheduled Permanent Departures or Unauthorized Absences.** Under emergency conditions, such as the sudden unscheduled permanent departure, death, or unauthorized absence of the custodian, the following actions will apply:

(1) (U) An immediate inventory of all COMSEC material will be initiated within 24 hours after the unauthorized absence, death, or sudden permanent departure of the custodian has been detected. The alternate custodian, or other properly cleared person, and a cleared witness will perform the inventory. This inventory will be recorded on an SF 153 (COMSEC Material Report), or equivalent for AKMS accounts, for all ALC 1, ALC 2 and ALC 6 material. ALC 4 and ALC 7 will be retained locally.

(2) (U) The resulting inventory report will be marked "Special Inventory" at the top of the SF 153 or AKMS equivalent and will contain the following comments: "This inventory is taken due to the sudden permanent departure, death, or unauthorized absence of custodian (name/rank). Request (unit) be notified ASAP of any discrepancies prior to the appointment of a replacement custodian." Furthermore, this report will contain all necessary remarks pertaining to discrepancies (if any) and be submitted to the COR for verification. The COR will verify the information and either provide the commander with a listing of all discrepancies or notification that the inventory matches the COR's records.

(3) (U) Upon receipt of the inventory verification from the COR, the commander will appoint a new custodian, who meets the COMSEC Custodian requirements, and submit a CARP to Tier 1. A second inventory will be taken in which the incoming custodian and a witness will sign. If the alternate custodian was the individual who completed the special inventory, and is subsequently appointed as custodian, an additional inventory report is not required. The appointment of any other individual will require that the procedures of paragraph 2.7 be followed.

(4) (U) If the account is an AKMS account, access to the system by the departed COMSEC Custodian must be deleted. See Chapter 6, Table 6-2, for instructions relating to deleting an individual from accessing LCMS.

## 2.9 RELIEF FROM ACCOUNTABILITY.

**a. (U) Unresolved Discrepancies.** The former COMSEC Custodian will not be relieved from accountability for accountable, COMSEC material, which is involved in any unresolved discrepancy.

**b. (U) Departure Prior to Clearance**. When a COMSEC Custodian departs an organization after the CCIR has been submitted, but before clearance is granted, the COR will request that the appropriate MACOM assist in getting the former custodian to reconcile all outstanding discrepancies. The commander of the COMSEC account assumes all responsibility of the COMSEC account if the former COMSEC Custodian is allowed to depart prior to clearance being granted by the COR.

**c. (U) Relief from Accountability**. The COMSEC account custodian will be granted relief from accountability for COMSEC material by CSLA after satisfactory evaluation of the incident reports, as directed in AR 380-40. In all cases of relief from SECURITY accountability, the following statement will be placed on file in the COMSEC account record: "The circumstances surrounding the loss of (identify material) have been considered and a determination has been made that a Request for Relief from Property Accountability (IS, or IS NOT) required."

**d. (U) Relief from Property Accountability.** Relief from COMSEC accountability by the COR is not relief from accountability for the loss, damage or destruction of Government property, as defined in AR 710-2 and AR 735-5. Reports of Survey, AR 15-6 Investigations, and other property accountability and responsibility may be required for the physical loss of COMSEC equipment, as prescribed in AR 735-5. COMSEC Custodians should seek advice and recommendations from Command S-4 staff elements and Property Book Officers.

## 2.10 MOVEMENT OF COMSEC ACCOUNTS.

(U) When an organization is moved between overseas and CONUS, between overseas commands, or within CONUS commands, the custodian will take the following actions:

### 2.10.1 (U) Traditional Account Custodian Actions.

**a. (U) Notification.** Notify the COR, supporting CLSF, all key CONAUTHs and the Defense Courier Service of the impending movement.

**b. (U) Disposition of Equipment.** Determine proper disposition for material held by Hand Receipt Holders.

**c. (U) Disposal of Equipment.** Properly dispose of material that will not be required at the new location.

**d. (U) Disposition of Material.** Determine if any of the COMSEC material will be transferred to a different account. If so, prepare and submit a Transfer Report (SF153) numbered in the 0001-4999 series. The report will include all accountable ALC 1 and 2 material being transferred. Submit a copy to the COR.

**e. (U)** Submit an updated CARP along with a current CFAR.

**f. (U) Prior to Shipment.** Conduct a local inventory of the COMSEC material which will be transferred to the new location and prepare a Change of Account Location Report, SF 153 (see paragraph 6.4.4). **Do not** send a copy of this inventory to the COR.

**g. (U) Receipt of Shipped Material.** When material arrives at the new location, perform a local inventory to verify receipt of all COMSEC material.

**2.10.2 (U) AKMS Account Custodian Actions.**

**a. (U) Notification**. Notify the COR, supporting CLSF, all key CONAUTHs and the Defense Courier Service of the impending movement.

**b. (U) Disposition of Equipment**. Determine proper disposition for material held by Hand Receipt Holders.

**c. (U) Disposal of Equipment**. Properly dispose of material that will not be required at the new location.

**d. (U) Disposition of Material.** Determine if the physical COMSEC material can be transferred to an existing COMSEC account. Depending on this decision, the following actions will be taken:

(1) (U) If the physical material is to be transferred to an existing COMSEC account, prepare and submit a Transfer Report (SF 153). The Transfer Report will include all accountable ALC 1, 2, and 6 material being transferred. Transmit the Transfer Report to the COR.

(2) (U) Update the Directory Service of location change.

(3) (U) Once the request for a COMSEC Facility has been approved, all physical COMSEC accountable material must be shipped via DCS or a properly cleared courier to the new approved COMSEC Facility.

(4) (U) The Cryptographic Ignition Key (CIK) associated with the Key Processor (KP) must be shipped in a separate container from the KP when being transported via DCS.

(5) (U) The removable hard drive from the LMD (contains the stored electronic key) must be handled as SECRET collateral. All non-COMSEC accountable material associated with the workstation must be sent to the new location IAW AR 380-5.

**e. (U) Prior to Shipment**. Conduct a local inventory of the COMSEC material which will be transferred to the new location, and prepare an inventory report (SF 153). **Do not** send a copy of this inventory to Tier 1.

**f. (U) Receipt of Shipped Material**. When material arrives at the new location, perform a local inventory to verify receipt of all COMSEC material.

**2.10.3 (U) COR Processing Actions.** The COR will perform the following processing actions:

**a. (U) Suspense**. Establish a 90-day suspense to allow the transferring organization to relocate.

**b. (U) Process Transfer Report.** Process the SF 153 Transfer Report if material is transferred to a new or existing account.

**c. (U) Notify the Service Authority**. Provide the modified CARP to the Service Authority for processing along with the COMSEC Facility Approval Request (CFAR) to establish a new account.

## 2.11 CLOSING OF COMSEC ACCOUNTS.

**2.11.1 (U) Commander's Actions.** When an account is to be closed, the commander will take the following actions:

**a. (U) Notification.** Notify CSLA by message or memorandum of the impending closure. The subject will read: "Request closure of COMSEC Account 5DEXXX." If COMSEC material held by the closing COMSEC account is to be transferred to a peer COMSEC account, then state so and provide the account number. Also, request relief from accountability for the COMSEC Custodian by name, rank, and Social

Security Number. An information copy will be forwarded to the CONAUTH, the Defense Courier Service, and the supporting CLSF.

**b. (U) Disposition Instructions.** Obtain disposition instructions for all COMSEC account assets from the CONAUTH. Destroy or transfer material as directed by the CONAUTH and submit appropriate SF 153s (0001– 4999 series), or AKMS equivalent, to the COR.

**c. (U) Disposition of Material.** Determine proper disposition for material held by Hand Receipt Holders.

**d. (U) Resolution of Incidents.** Resolve any open COMSEC Incidents.

**e. (U) Relief from Accountability.** Only after all COMSEC material is properly disposed of and all Reportable COMSEC Incidents are resolved, will the Service Authority issue a closure message/memorandum, granting relief from accountability to the COMSEC Custodian. Semiannual Inventory Reports (SAIRs) continue to be required until all assets have been disposed of properly and the account has reached a "zero balance."

**2.11.2 (U) COR Procedures Upon Closure of COMSEC Accounts.** The COR will initiate the following procedures upon the closure of a COMSEC account:

**a. (U) Notify Shippers**. Upon receipt of the request to close an account, notify all shippers of impending closure and direct that all shipments be stopped in order to facilitate closure.

**b. (U) Provide Asset Listing**. If requested, the COR will provide an asset list to closing accounts.

**c. (U) Open COMSEC Incident Cases.** Check account records for any open COMSEC Incident cases.

**d. (U) Transactions**. Process all transactions as received until account balance is at zero.

**e. (U) Closure and Relief from Accountability.** Forward a message/ memorandum stating the account is closed and relieve the COMSEC Custodian from accountability.

**2.11.3 (U) Closing of Accounts Due to Inactivity.** CSLA monitors the degree of activity within all COMSEC accounts. When an account has shown no activity for 12 months, CSLA will advise the unit commander, through the MACOM, that the COMSEC account is subject to being closed due to inactivity. The unit commander will be given 60 days to justify a continuing requirement for the account. If none is provided, CSLA will provide disposition instructions for the CMCS accountable material and close the account.

## 2.12 CONTINGENCY DEPLOYMENT OF A COMSEC ACCOUNT.

**(U) Neither CSLA nor a deploying unit makes the final decision that the unit shall deploy with or without its COMSEC account. Rather, this decision is made at the highest levels of the chain-of-command (General Officer level) through consultation and coordination between the overseas Theater Commander and the unit's MACOM. However, *unless specifically directed otherwise by a competent authority*, any unit alerted for deployment will deploy with all its MTOE authorized personnel and equipment, including their COMSEC account.**

(U) During times of national emergency, wartime buildup, or as directed by a National Command Authority, mission requirements may require COMSEC accounts to be temporarily relocated to different geographical locations for extended periods. When faced with these circumstances, commanders and COMSEC personnel will refer to the following procedures:

**2.12.1 (U) Traditional COMSEC Account Contingency Deployment**. The custodian will follow paragraph 2.10.1 a-g for traditional (non-automated) COMSEC accounts, as well as the additional requirements listed in paragraph 2.12.3 below.

**2.12.2 (U) AKMS COMSEC Account Contingency Deployment**. The custodian will follow paragraph 2.10.2 a-g for AKMS COMSEC accounts, as well as the additional requirements listed in paragraph 2.12.3 below.

**2.12.3 (U) Additional Requirements for Deploying COMSEC Accounts.** Each deploying unit must prepare a detailed SOP for the deployment and operation of the COMSEC account at the deployment site, tailored to its own unique situations. All COMSEC accounts, whether traditional or automated, will additionally perform the following steps when deploying under the contingency conditions described in paragraph 2.12 above.

(1) (U) The unit will submit a new DCS Form 10 when arriving at the new location and provide a forwarding DCS station address to CSLA Key. The account will NOT change account numbers.

(2) (U) The custodian must review the account's key material assets and provide CSLA (COR-Key) a listing of the short titles the account will be taking, and a listing of the short titles of material to be transferred or destroyed. The CSLA Key Manager will stop shipment on short titles that will not go forward.

(3) (U) CSLA will re-direct the shipment of future keying material to the DCS station closest to the deployment location once the custodian has provided that location. When the deployment location is unknown before departure, the custodian will notify the Key Manager after arrival at the new location so that future material can be re-directed to that location.

(4) (U) For material that will go forward with the deploying account, the commander must decide the method of transportation (i.e., will the material be packaged and escorted [courier] at the time of the unit's deployment by COMSEC personnel for control purposes or, will it be shipped separately to the new destination via DCS). If the material is to be sent via separate shipment through DCS, the custodian must contact a supporting COMSEC account in the deployment area ***prior to deploying – and in advance of shipment***. The custodian will coordinate with that COMSEC account to receive and secure the incoming DCS shipment, and hold it, *unopened*, until arrival of the deploying unit.

(5) (U) When preparing COMSEC material for shipment, whether by escort or DCS, all material must be packaged properly (double wrapped) and addressed/ identified as the property of the owning (shipping) account. This will preclude the shipment from arriving at the distant "holding account" and being mistakenly opened.

(6) (U) If the deployed unit establishes a strategic/**fixed** COMSEC Facility at the deployment location, a new CFAR is required once the account has arrived at its new location. Under paragraph 2 of the new CFAR being submitted, the custodian must indicate that the account has been deployed by providing the following information:

- Account Number –5XXXXX – Deployed
- Location: (If not classified)
- Type Request: Update – Tactical, GSA Approved Security Container/room or vault.

The COR will institute a 90-day suspense allowing for the re-location of the COMSEC account IAW paragraph 2.10.3a.

(7) (U) While in deployment locations wherein circumstances dictate that combat/combat support units operate their COMSEC accounts from **mobile** facilities under dynamic tactical conditions, a CFA is not required. The local command security officer will be responsible for ensuring adequate security measures are employed to protect such facilities at the deployment sites, consistent with local contingency conditions. The use of barrier material, barbed wire, concertina wire, armed guards, etc. is encouraged. Because of the fluid situations that come from a mobile operational status, it would be

impossible to predict every scenario. However, the custodian **must** become familiar with paragraphs 5.7 through 5.10 of this TB so that he/she can assist the commander in making the best decisions possible to ensure the security, custody and accountability, physical protection, access control, storage requirements, and surveillance of the account and the COMSEC material.

**2.12.4 (U) CSLA Responsibilities to the Deployed Account.** CSLA will continue to provide support to the deployed COMSEC account. The following are areas CSLA will be responsible for, but not limited to, during the time an account is deployed:

- Process all accounting transactions
- Ensure shipment of material
- Provide and reconcile SAIRs/CCIRs
- Monitor transactions of material

## 2.13 UNIT DEPLOYMENT WITHOUT A COMSEC ACCOUNT.

**2.13.1 (U) Mission Support.** During contingency operations, some Army units are deployed for short durations (non-PCS deployments) with orders not to bring their organic COMSEC accounts. Under these circumstances, COMSEC support is provided by established COMSEC support facilities at the distant location. When a unit is deployed without its COMSEC account, and the COMSEC account is left unmanned and inactive for an extended period at its home station, there are two options available to the commander. It is strongly recommended that commanders and COMSEC account personnel follow these guidelines to prevent Reportable COMSEC Incidents from occurring.

**a. (U)** If the unit is expected to be deployed in excess of 12 months, or if the commander decides for other reasons the account is to be permanently closed, account closure procedures will be followed IAW with paragraph 2.11.

**b. (U)** When the deployment period is expected to be less than 12 months, the account may be placed in a "suspended" status until the unit's return and reactivation of the account.

**2.13.2 (U) Suspension of a COMSEC Account.** When a unit is to be deployed without the COMSEC account, plans and coordination must be made for disposition of the COMSEC account's material and LCMS Workstation prior to the COMSEC Custodian's departure to the deployment location. When the commander's decision is to retain the COMSEC account in a non-operational suspended status, the custodian will take the following actions:

**a. (U) Notification.** The COMSEC Custodian must make all required notifications **as soon as possible** after receiving knowledge of impending unit deployment without its COMSEC account.

(1) (U) Notify all applicable Controlling Authorities (CONAUTHs), supporting CLSF, and the COR, in writing via memorandum, message, e-mail, etc., of the pending unit deployment and the command decision to place the account in a non-operational suspended status. The subject will read: "Request for Non-Operational Suspension of COMSEC Account 5DEXXX." Provide as much detail as possible regarding the deployment and circumstances pertaining thereto.

(2) (U) The unit must contact its servicing DCS station as soon as possible after notification of a deployment without the COMSEC account. DCS requires a "trusted agent," such as the unit commander or the COR, to officially request suspension of material delivery to the account. This will prevent frustration in having to return physical material shipments to senders.

**b. (U) Disposition of COMSEC Material and Equipment.** All CMCS accountable material held in the COMSEC account must be destroyed or transferred to a Peer COMSEC account; leaving the account at a "zero balance" before the custodian departs the home station.

(1) (U) Obtain disposition instructions for all COMSEC account assets from the CONAUTH(s). Destroy or transfer material as directed by the CONAUTH and submit the appropriate LCMS Workstation electronically generated reports (or SF-153s 0001– 4999 series reports for manual COMSEC accounts) to the COR.

(2) (U) The KOK-22A plays an integral part in electronic signatures being applied to AKMS transactions sent to the COR. For this reason, the KOK-22A and associated keys should be the last items transferred from an AKMS account before reaching zero balance. Transfer the KOK-22A and associated keys to another COMSEC account for holding purposes as designated by the cognizant commander in the chain of command. The KOK-22A must remain in an operational status to allow its own Transfer Report Initiating (TRI) to be correctly prepared and sent to the COR. **DO NOT ZEROIZE THE KOK-22A AFTER COMPLETING THE FINAL TRANSACTION OF TRANSFERRING THE KOK-22A.**

(3) (U) In those instances when re-certification of the KOK-22A will be required during the period when the unit is deployed, the CSLA KOK-22A Item Manager will provide special instructions for returning the KOK-22A to Lackland AFB, TX, for re-certification prior to the unit's deployment. The KOK-22A certification date is determined by viewing the battery installation date on the rear side of the KOK-22A. The re-certification date of the KOK-22A is approximately three (3) years from the installation date of the battery.

**(U) The COMSEC Custodian must contact the CSLA KOK-22A Item Manager prior to taking any action to transfer the KOK-22A to a holding account or to the depot at Lackland, AFB.**

(4) (U) Ensure the PBO or other responsible rear detachment personnel have control of classified LMD components and ancillary LMD items. Local COMSEC Management Software (LCMS) Workstation components (except KP and associated keys) are Property Book items and may be maintained (stored) as classified and high-dollar items by rear echelon personnel during the unit's deployment. It is recommended that the entire LCMS Workstation be stored as a single AN/GYK-49 system (excluding the KOK-22A) to avoid loss and to facilitate re-activation of the account upon the unit's return to home station.

**2.13.3 (U) Unit Return to Home Station.**

**a. (U) Notification.** The COMSEC Custodian must make all required notifications after receiving orders regarding the unit's impending return to home station. Two (2) months prior to the deployed unit's anticipated return, the COMSEC Custodian, or other cognizant COMSEC personnel, will take the following actions:

(1) (U) Contact the CSLA COR and KOK-22A Item Manager for coordination and procedures required for returning the COMSEC account to an operational status. Through this coordination, the holding account will be directed by CSLA to transfer the same serial numbered KOK-22A and keys back to the COMSEC account upon the unit's return. In cases where, prior to deployment, the CSLA KOK-22A Item Manager directed the KOK-22A be sent to the depot at Lackland, AFB, CSLA shall take action to have a re-certified KOK-22A sent to the unit via DCS.

(2) (U) In addition, the unit will provide information to the CSLA COR account manager and CSLA Audit section to confirm that the location, technical details, and physical security, as shown on the CFAR and authorized by the CFA, have not changed during the period of deployment. The COR will validate the custodian's and/or alternate custodian's current status. Changes to the CFAR, CFA, or CARP (including personnel training for SCCC and LCMS) will be reconciled with CSLA prior to the suspended status being lifted. The CSLA Audit section and COR will assist the unit to ensure that an accurate

CFAR, CFA, and CARP are in place at the time of the unit's return to home station.

(3) (U) Prior to the deployed unit's anticipated return, the COMSEC Custodian, or other cognizant COMSEC personnel, will contact all applicable CONAUTHs and the servicing DCS station to initiate steps for returning the COMSEC account to an operational status.

**b. (U) Return of COMSEC Account Material and Equipment.**

(1) (U) Upon direction from CSLA, the COMSEC account holding the accountable COMSEC material and/or the KOK-22A will transfer the remaining material, the same serial numbered KOK-22A, and associated keys back to the returning COMSEC account.

(2) (U) The unit COMSEC Custodian will arrange with the PBO to have the remaining stored LCMS Workstation components hand-receipted to the account in order to re-configure them into an operational LCMS Workstation.

(3) (U) The custodian will notify the COR Account Manager when the account has achieved full operational status and is prepared to receive CMCS-accountable material. The COR will provide this information to the CSLA Audit Section.

**2.13.4 (U) CSLA Responsibilities:**

(1) (U) NOTIFY THE NSA TO SUSPEND SHIPMENTS TO THE ACCOUNT UNTIL FURTHER NOTICE.

(2) (U) NOTIFY THE NSA CENTRAL FACILITY (CF) TO BLOCK OR DISABLE THE ACCOUNT'S MAILBOX, PRECLUDING EKMS TRANSACTIONS FROM SETTING IN THE BOX FOR EXTENDED PERIODS WHILE THE UNIT IS DEPLOYED AND THE ACCOUNT IS SUSPENDED.

(3) (U) KEEP THE ACCOUNT OPEN IN CSLA RECORDS BUT IN A SUSPENDED STATUS UNTIL FURTHER NOTICE.

(4) (U) ENSURE CSLA AUDIT SECTION IS AWARE OF THE SITUATION AND OF ANY CHANGES OCCURRING AS THE MISSION PROGRESSES AND/OR IS COMPLETED.

(5) (U) MONITOR AND ASSIST THE UNIT UPON RETURN TO ENSURE AN ACCURATE CARP IS APPROVED AND ON FILE, AND THAT QUALIFIED PERSONNEL ARE STILL AVAILABLE AND PREPARED TO MAINTAIN THE COMSEC ACCOUNT (INCLUDING SCCC AND LCMS TRAINING).

THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY

# CHAPTER 3

# SUPPLY AND CONTROLLING AUTHORITY PROCEDURES

## 3.1 IDENTIFYING COMSEC MATERIAL.

**a. (U) ARKAG 1. COMSEC Material Management Data.** This document listed management data for all COMSEC material; however, the ARKAG1 has been eliminated with the implementation of Tier 1. The function of the ARKAG1 is now an automated service. Manual accounts or Peer accounts must call the item manager for any information in question.

**b. (U) The Federal Catalog (FEDLOG).** This file lists catalog data for all equipment.

**c. (U) Critical Data Elements:**

(1) (U) The Accounting Legend Code (ALC) identifies how an item must be accounted for in the CMCS (reference paragraph 4.2 of this TB for a listing of the ALCs).

(2) (U) Controlled Inventory Item Code (CIIC). The CIIC for COMSEC equipment is listed in the FEDLOG. A code number of “9” in the FEDLOG CIIC column means the equipment is CCI. A code of “U” is for unclassified.

(3) (U) Source of Supply (SOS). SOS is listed in the FEDLOG.

## 3.2 REQUISITION FUNDING AND RETURNS.

(U) The current Standard Army Stock Fund System is in the process of being transitioned to the Army Working Capital Fund (AWCF). This transition will affect all COMSEC accounts as it applies to requisitioning, funding and turn-in of COMSEC secondary items, and is being accomplished incrementally installation by installation. Concurrently, CSLA is transitioning from the Army COMSEC Commodity Logistics, Accounting and Information Management System (ACCLAIMS) to the Commodity Command Standard System (CCSS). This will affect processing of transactions for secondary items and end items, including classified equipment and repair parts. Until all procedural changes have been made to ensure compatibility between the various systems, the following requisition, funding and turn-in procedures will continue to be valid. CSLA will notify COMSEC Custodians when revised procedures become effective. If custodians encounter any problems, contact CSLA for assistance. The customer service number is 1-800-662-2123.

**3.2.1 (U) Requisitions.** Class VII End Items, COMSEC Key (except FORTEZZA cards), and publications obtained through CMCS channels are free issue to Army units and do not require funded requisitions. Likewise, returns for similar items through the CMCS do not receive monetary credit.

**a. (U)** COMSEC secondary hardware items are no longer free issue. Identification of COMSEC items at unit level, which require funding and those that are free issue, can be accomplished by review of the Material Category Structure Code (MATCAT) on the Army Master Data File (AMDF) portion of the FEDLOG. CSLA-managed items with a Numeric Code of “2” in the SECOND position of the MATCAT require funded requisitions.

**b. (U)** COMSEC Custodians are responsible for ensuring that Operations and Maintenance (O&M) funds are available to reimburse the supporting wholesale stock fund for material prior to requisitioning. Custodians who are unfamiliar with local funding/billing procedures are encouraged to contact their respective budget officers and supporting resource management office.

**c. (U)** Detailed information on the preparation and coding of requisitions is contained in AR 710-2 and AR 725-50. COMSEC accounts, which submit requisitions directly through normal supply channels, are responsible for application of correct MILSTRIP funding/billing data.

**d. (U)** All requisitions received by CSLA for secondary items must contain standard MILSTRIP funding/billing data as follows:

(1) (U) *Fund Code* - XP (see AR 725-50).

(2) (U) *Signal Code* - (See AR 725-50 for the appropriate Signal Codes for shipping/billing instructions.)

**e. (U)** The XP fund code will indicate to CSLA that fund availability has been verified. It also signifies that billing will be accomplished manually using Standard Form 1080 billing procedures instead of the automated inter-fund billing system. The standard financial system requires a Department of Defense Activity Address Code (DODAAC) to identify the appropriate F&AO to which billings will be sent. The DODAAC in the CARP, on file in Tier 1, will be used by USACECOM Finance Office to determine the customer's servicing F&AO. Therefore, it is imperative that COMSEC Custodians periodically review the Department of Defense Activity Address Directory (DODAAD) to verify that assigned unit/account DODAACs are valid and have not been changed or deleted from the DODAAD. If the DODAAC recorded on the CARP is incorrect, immediately submit a modified CARP to CSLA.

**3.2.2 (U) Customer Returns.** Turn-in credit will be given to COMSEC accounts, as explained in the following paragraphs, for classified COMSEC secondary items managed within the CMCS only. Unclassified/CCI COMSEC material will be returned by the PBO; other supply accounts will be returned through standard logistics channels using the material returns program procedures specified in DA Pam 710-2-1.

**a. (U)** Funding/billing data is not required on Army SF 153 turn-in documents. CSLA will assign fund code "XP" on all turn-ins for classified items received at the COMSEC depot activity. This applies only to Army COMSEC accounts (account numbers beginning with a "5").

**b. (U)** The standard financial system requires billing/credit transactions to be processed as single-line entries. Therefore, all customer turn-ins for funded COMSEC material must be prepared as single-line documents. This means that only one short title may be listed on the SF 153. In addition, if the items being returned are technically/operationally classified into more than one condition code, a separate SF 153 must be prepared for each. FOR EXAMPLE: If a unit is turning in 10 printed circuit boards (PCB), Short Title E-ABC, two of which are condition code A (Serviceable), and the remaining eight are condition code F (Unserviceable/ Reparable), two separate SF 153s are required. This requirement for single-line SF 153s does not apply to items for which monetary credit is not authorized, such as free issue items, obsolete items, and uneconomically reparable items.

**c. (U)** Monetary credit will not be granted for material turned in to Tobyhanna Army Depot if the wholesale stockage levels are in an excess position. Wholesale inventory managers have the authority and discretion to deny credit to customers unless there is a current or projected need for the material returned from field units.

**d. (U)** The amount of credit provided will be based on material condition upon receipt, as determined by depot technical inspection. Calculation of the appropriate monetary credit will be accomplished using standard Army formulas provided by HQDA, within the serviceability criteria/requirement guideline. Computed amounts will then be forwarded to the applicable servicing F&AO for credit to the customer's account using the same procedures explained for billing transactions in paragraph 3.2.1. Credit formulas for unserviceable items are subject to periodic adjustment based on actual repair/replacement and labor costs.

**e. (U)** Regardless of other considerations, turn-in credit will not be allowed for any unserviceable returns that do not meet economical repair criteria and maintenance expenditure limitations for COMSEC material.

**3.2.3 (U) Customer Assistance.** Questions regarding the contents of this section, and assistance in stock fund matters which cannot be resolved locally, may be addressed by contacting CSLA by telephone at Toll Free 1-800-662-2123, or in writing.

## 3.3 REQUISITIONING OF COMSEC MATERIAL.

**3.3.1 (U) General COMSEC Requisition Procedures and Applicable Publications.**

**a. (U) Classified COMSEC Equipment.** COMSEC Custodians will requisition these items through the CMCS. Requisitioning policy is in AR 710-2. Requisitioning procedures are in DA PAMs 710-2-1 and 710-2-2.

**b. (U) Controlled Cryptographic Items (CCI).** CCI will be requisitioned and locally accounted for on property books or stock record accounts IAW AR 710-2. Management and accountability of CCI is a standard logistics function under the control of Installation Accountable Officers and unit Property Book Officers (PBOs). CCI end item serial numbers are reported in the Controlled Cryptographic Item Serialization Program (CCISP) IAW AR 710-3. Selected CCI components require Selected Item Management System-Expanded (SIMS-X) reporting IAW AR 710-3.

**c. (U) Unclassified COMSEC Equipment.** Unclassified COMSEC equipment items which are **NOT** designated CCI, such as the NAVSTAR Global Positioning System (GPS) and the new family of Secure Telephone Equipment (STE), will be requisitioned through normal supply channels and will be accounted for and controlled as “Sensitive Items,” as prescribed in AR 710-2. The loss or theft of unclassified COMSEC “sensitive items” requires investigation and reporting per AR 735-5.

**d. (U) National Security Agency (NSA)-Produced COMSEC Publications (KAMs, KAOs, etc.).** These publications are requisitioned by COMSEC Custodians through the CMCS (see subparagraph 3.3.2.a.).

**e. (U) COMSEC Key.** COMSEC key is requested by the CONAUTH. Procedures for requesting the establishment of a Cryptonet are covered in paragraph 3.6.

**3.3.2 (U) Initial Issue of COMSEC Publications.**

**a. (U) NSA-Controlled COMSEC Publications.** Traditional accounts requisition these publications through COMSEC logistics channels using the appropriate requisition form (DD Form 1348). AKMS accounts will order the publications through their LCMS Workstation from the supporting CLSF or COR, as applicable. The requestor will receive the basic publication plus all printed amendments and changes with the initial issue. Subsequent editions, amendments, and changes will be automatically issued to COMSEC accounts, which are charged with the basic publication (and are authorized the level of maintenance manual involved). Publications will be issued by the supporting CLSF for OCONUS or by CSLA for CONUS. The lateral transfer of NSA-controlled COMSEC publications from one COMSEC account to another is not authorized without prior approval of the supporting CLSF or CSLA.

**b. (U) Army COMSEC Publications.** Army COMSEC Publications are requisitioned through the Standard Army Publications System (STARPUBS). Army publications dealing with COMSEC policy, procedures, equipment operation, and maintenance (i.e., Technical Manuals [TMs] and Technical Bulletins [TBs]) are automatically issued by updating the DA Form 12 Series. This will establish an account on the initial distribution list for new/revised publications that have not already been distributed within the Army. Local publication channels can obtain existing publications via the submission of DA Form 4569.

**c. (U) NSA Limited Maintenance Manuals (LMM).** LMMs are NSA-produced maintenance manuals for CCI equipment. LMMs are requisitioned through STARPUBS. LMMs differ from the NSA KAMs in that they are not controlled within the CMCS and are not assigned an ALC (see paragraph 3.3.2.b).

**d. (U) NSA-Published Policy and Doctrine.** The National Security Agency has produced several Non-Cryptographic Operational General Publications (NAG), National Security Telecommunications and Information Systems Security Instructions (NSTISSI), Committee on National Security Systems (CNSS), and Information Assurance Directorates (IAD) policies and doctrine that contain operational security doctrine and procedures for various COMSEC devices in the Army inventory. COMSEC accounts are required to maintain a library of these documents applicable to their unit operations, provided they have been approved by HQDA for Army use. These Army-approved documents are not available for distribution through STARPUBS; however, they are locally reproducible to satisfy internal distribution requirements. Due to the continuing growth in the number of these publications, CSLA will list the applicable documents in their newsletter, The COLT, and will provide regular updates announcing new documents that have been approved by HQDA and are available for issue from CSLA.

(U) Army units are prohibited from acquiring or using NSA publications that have not been approved for Army use by HQDA.

**3.3.3 (U) Identification Plates/Labels.**

**a. (U) COMSEC End Items and Major Components.** All COMSEC end items and major components are identified with permanently affixed Identification (ID) plates containing short titles/nomenclatures, serial numbers, and security classification (if applicable). In addition, some items, as prescribed by equipment TMs and NSA publications, include labels or decals that identify items as CCI and/or show which modifications have been applied to specific items of equipment.

**b. (U) Serial Numbers.** Identification plates almost always have serial numbers on them. Other labels do not reflect serial numbers. Tobyhanna Army Depot (TYAD) manufactures ID plates upon request from CSLA. Other labels are assigned National Stock Numbers (NSNs) and may be requisitioned just like any other expendable supply item. These labels are listed in equipment TMs and are requested on DA Form 2765-1 from local Supply Support Activities (SSA).

**c. (U) Lost, Damaged, Destroyed, Mutilated, or Disfigured/Illegible Appliqués.** Whenever the required "appliqués" (data plates/labels) become lost, damaged, destroyed, mutilated, or disfigured/illegible, they must be immediately replaced. COMSEC Custodians (for classified equipment) and Accountable Officers (for CCI) are responsible for ensuring that action is taken to maintain the proper identity of all COMSEC material.

**d. (U) Replacement Labels/Plates.**

(1) (U) To obtain replacement identification plates or Printed Circuit Board (PCB) ID labels for COMSEC material, send a memorandum or electronic message to the POC listed in Appendix F. *Serial number replacement plates or labels for PCBs are replaced only when authorized maintenance technicians open equipment. The replacement of PCB plates/labels will be accomplished* ***only*** *by the COMSEC maintenance personnel authorized by the Source, Maintenance, and Recoverability codes, as shown in the applicable equipment TMs.*

(2) (U) Include the following information in your correspondence:

(a) (U) Short title/end item nomenclature, serial number(s), and COMSEC account number/DODAAC.

(b) (U) A short justification for the request explaining why the ID plates/labels need to be replaced.

(c) (U) If the serial number is not known, your request for a new serial number should contain the following statement: "A complete audit of records at this account has been made and there is no record of the original serial number available for this equipment."

(3) (U) When preparing a request for a new ID plate/label, the following certification statement is required: "I certify that none of the COMSEC items requiring ID plates or labels were fabricated, or if any items were fabricated, it was done with prior written approval of CSLA."

(4) (U) The Unit Commander **must** sign the certification. Upon receiving a request for ID plates, CSLA will issue new ID plates with the original or new serial number permanently inscribed. Upon request, instructions will also be provided on how to requisition replacement labels and decals through the supply system.

(5) (U) Users experiencing difficulty in obtaining replacement ID plates or labels should telephone CSLA, 1-800-662-2123.

**3.3.4 (U) Equipment Alteration.** See paragraph 4.18 of this TB.

## 3.4 NEED FOR CRYPTOSYSTEMS AND AUTHENTICATION SYSTEMS.

**3.4.1 (U) Information Security.**

(U) Cryptosystems provide security by preventing electronically transmitted information from falling into the hands of unauthorized persons. Machine cryptosystems and certain "one-time" cryptosystems are the most secure methods of protecting electronically transmitted information. Manual and auto-manual cryptosystems are used to protect electronically transmitted information only when machine systems are unavailable.

**3.4.2 (U) Authentication Systems.** Authentication systems provide a defense against enemy intrusion into communications nets. These systems are also used to establish the authenticity of stations, communicators, or communications.

**3.4.3 (U) Operations Security (OPSEC).** Properly used cryptosystems and authentication systems are necessary to maintain adequate OPSEC within a command.

**3.4.4 (U) Approved Systems.** The **only** cryptosystems and authentication systems approved for Army use are those systems as outlined below:

**a. (U)** Produced by the NSA and obtained through the procedures described within this chapter.

**b. (U)** Commercial Off-the-Shelf (COTS) Systems approved by the NSA/DA for local purchase under the Commercial COMSEC Endorsement Program (CCEP). See AR 710-2, Chapter 1.

**c. (U)** Electronic key generated and distributed using NSA-approved key generating systems.

**3.4.5 (U) Selection and Use.** For assistance in the selection and use of manual cryptosystems and authentication systems, contact CSLA. See Appendix F for POC information.

(1) (U) Users of each cryptosystem and authentication system will become familiar with the system's capabilities and limitations, and have a thorough knowledge of the appropriate operating instructions.

(2) (U) Detailed operating instructions normally accompany each copy of manual systems. The NSA, in the cryptosystems Operating Instructions (KAO), Limited Maintenance Manuals (LMM) and Army Operator's Technical Manuals I, publishes detailed instructions for each machine cryptosystem. An index of KAOs, LMMs and Army COMSEC Publications is listed in DA Pam 25-35.

## 3.5 CRYPTONETS.

**3.5.1 (U) Cryptonet Elements.** Establishing a cryptonet involves identifying those individuals and/or operating elements that must intercommunicate in a secure mode. In order to intercommunicate, all cryptonet members must possess compatible equipment, as well as the

associated key. Cryptonet planning is conducted in conjunction with communications network planning to ensure compatibility and interoperability with joint organizations, as well as Army Commands. CONAUTHs will give consideration to the employment of electronic key and the implementation of electronic re-key procedures. When electronically generated key is not used, the CONAUTH must send written justification to the Service Authority explaining why they are requesting hard copy key. This will limit hard copy key products to the minimum essential for mission accomplishment.

**3.5.2 (U) Types of Cryptonets.** The CONAUTH must consider which type of cryptonet (for example, operational or contingency) will be most economical in terms of production, distribution, storage, and destruction costs. With the exception of irregularly superseded key (such as one-time pads), key for operational nets is re-supplied as directed by the CONAUTH. Irregularly superseded key is re-supplied upon request of the CONAUTH. Key will be used as follows*:*

**a. (U) Operational Key.** Operational key will be used for routine day-to-day operations.

**b. (U) Contingency Key.** Contingency key will be used for operations that occur infrequently (exercises less frequent than one each month). The use of operational key to secure infrequent operations is discouraged, except as explained in the following paragraph, because it will result in **NEEDLESS** and **COSTLY** destruction of unused key and it is manpower intensive.

**c. (U) Use of Operational Key for Contingency Purposes.** One or more editions of operational key may be identified for training/exercise use by the CONAUTH. The CONAUTH may also choose to change the status of an operational key to contingency for future use instead of cancellation when a net has been discontinued. Both of these actions must be coordinated with CSLA Key Management and the NSA. The CONAUTH may change the key back to an operational status at a future time, if required. The CONAUTH is responsible for advising all users and CSLA of disposition instructions of unused, cancelled, or superseded key.

**3.5.3 (U) Cryptonet Size.** The size of the cryptonet will be as small as operationally feasible for the types of organizations and cryptosystems requiring hard copy key. The CONAUTH will always determine the number of holders and copy count requirements for key.

**3.5.4 (U) Cryptonet Expansion.** All cryptonets established will consist of essential members **only** and have a key copy count sufficient to satisfy the secure communications requirement. Additional copies of key to be used for possible expansion of Army cryptonets will not be held by a CLSF unless directed by a higher headquarters that has received prior approval from the CONAUTH and the NSA*.*

## 3.6 ESTABLISHMENT OF CRYPTONETS.

**a. (U) Requests for Establishment of Cryptonets (Physical Key).** Requests for establishing machine or auto-manual cryptonets (including requests for approved cryptosystems and authentication systems) will be submitted via message by the commander of the requesting activity. These requests, in the form of a memorandum or message, will be submitted to CSLA with the information addressees of the NSA, Y132 and the requestor's next higher headquarters listed. For KG-84 key, provide this information to the NSA, ATTN: Y271 and Y132. See Appendix F for POC addresses.

(1) (U) Requests for manual cryptosystems will be submitted to the action and information addressees listed in the preceding paragraph. This includes OPCODES, One-Time Pads (OTP), Authentication Systems, etc.

(2) (U) AKMS accounts will utilize the attributes in the LCMS. Refer to the LMD/KP Operators Manual.

**b. (U) Standard Request Form**. Requests for physical key will contain the following information, as appropriate. Message requests for classified key will be classified as CONFIDENTIAL due to the compilation of information. Request for UNCLASSIFIED key will be marked and handled as FOUO.

(1) (U) *Type of Key.* (Refer to figure 3-1): Electronic keying/re-keying techniques

will be employed to the maximum extent feasible.

(a) (U) Indicate type of key required (KG-84C, KY-57/58, etc). If the request is for the Traffic Encryption Key (TEK) transition training tape, provide the number of months the tape will be required. The tape production will be scheduled for the requested period only.

(b) (U) If the request is for Key Encryption Key (KEK) tape, specify the reason for KEK tape instead of local generation of KEK (e.g., KG-83 is not available for generation of KEKs).

(2) (U) *Designated CONAUTH.* Include CONAUTH message address, a point-of-contact, e-mail address and telephone number.

(3) (U) *Nature of Request.* Indicate nature of request (i.e., new equipment or establishment of cryptonet).

(4) (U) *Key Usage.* Indicate key usage: National Emergency Operations (NEO), State Emergency support/Civil Action, etc. For machine or auto-manual cryptosystems, provide a brief statement describing the scenario under which the requested key is to be used. For manual cryptosystems, provide a detailed description of the requirement.

(5) (U) *Classification.* Indicate the classification of information to be encrypted (CONFIDENTIAL, SECRET, or TOP SECRET).

(6) (U) *Number of Copies.* Indicate the required number of editions and the total copy count per edition. Also, when requesting establishment of a cryptonet, indicate the canister configurations requested. See paragraph 4.8.1a and b for canister configuration.

(7) (U) *COMSEC Account Numbers.* Indicate the COMSEC account number(s). Also, include the number of copies to be shipped to each account.

(8) (U) *Delivery Date.* Indicate the Required Delivery Date (RDD). Normal production lead-time is 120 days from receipt of the request by the NSA.

(9) (U) *Purpose of Operation.* Include information (such as exercise name and dates or dates and length of the on-the-air test) to assist in identifying when the material will be used.

(a) (U) CSLA, the NSA (Y13), and the supporting CLSF (when applicable) will be notified when a newly established operational cryptonet (using regularly superseded key) has started operations. This notification allows the automatic re-supply of key to begin (see Figure 3-1).

(b) (U) CSLA and the NSA will also be notified each time an edition of any contingency key is implemented. Contingency key will only be re-supplied when the CONAUTH requests it.

(10) (U) *Net Structure and Operation.* Indicate net structure and operation, and state if cryptonet is point-to-point or netted.

(11) (U) *Short Title.* Indicate the Short Title of the key to be replaced, if applicable.

(12) (U) *Quantity of Crypto-equipment.* For machine cryptosystems, indicate the total quantity of crypto-equipment on-hand that will use the key requested.

(a) (U) If the crypto-equipment is not on-hand, show the equipment delivery date as established by the CSLA. If the delivery date is more than four months away, the key will not be requested. Also, if the communications equipment used in support of the crypto-equipment is not on-hand, and is not due to be delivered within four months, the key will not be requested.

(b) (U) For One-Time Tapes/Pads/Disks, indicate whether the system is a point-to-point system or a family-type system (e.g., a 5-way family system

would consist of five editions, each edition consisting of one encipher and four decipher pads/tapes/disks). Indicate type of circuit (full-duplex, half-duplex, etc.).

(13) (U) *Emergency Reaction Force.* Indicate if the unit is part of a Command Emergency Reaction Force.

(14) (U) *Validation by Higher Headquarters.* Include a statement to verify the higher headquarters has validated the need for the cryptonet.

**c. (U) AKMS Accounts.** AKMS accounts will send requests using the free form text directly through the message server. Refer to Chapter 6 of this TB for additional key issues pertaining to AKMS.

*Free form text messages will adhere to the standard English rules of convention (e.g., spacing, punctuation, grammar). Failure to construct a legible message may result in the request being returned to the sender unfulfilled.*

This is an example of a message request to establish a cryptonet. Content will vary according to local requirements. **Classification is for example purposes only**.

```
                              ***CONFIDENTIAL***

01   02   081241Z   FEB  03   RR   RR   CCCC      AA   ZYUW    TTC-1
NO
       FROM   CDR PIRMASENS GE //5A0419//
       TO     DIRCSLA FT HUACHUCA AZ//SELCL-ID-KEY//
              DIRNSA FT MEADE MD //Y132//
       INFO   NCTAMS LANT NORFOLK VA //159039
C O N F I D E N T I A L
SUBJECT:  ESTABLISHMENT OF CRYPTONET (U)
A. (U) TB 380-41 PROCEDURES FOR SAFEGUARDING, ACCOUNTING, AND SUPPLY
CONTROL OF COMSEC MATERIAL
1. (C) THIS PARAGRAPH IS CONFIDENTIAL DUE TO COMPILATION IAW CHAPTER 3,
REFERENCE A.  THIS ACTIVITY HAS A REQUIREMENT TO ESTABLISH A CRYPTONET
USING APPROVED KEY.
   A. (U) TYPE OF KEY:  KG-84() OPERATIONAL OTAR KEY KEYTAPE, TENNLEY
(KEY ENCRYPTION KEK WITH WEEKLY OTAR, QUARTERLY CRYPTOPERIOD, ANNUAL
EDITION SUPERSESSION).
   B. (U)  CONAUTH:  CDR PIRMASENS GE //5A0419//, DSTN/STU-III: XXXXX.
   C. (U)  NATURE OF REQUEST:  NEW REQUIREMENT.
   D. (U)  KEY USAGE:  OPERATIONAL.
   E. (U)  CLASS:  TOP SECRET.
   F. (U)  COPY COUNT:
        (1)  NUMBER OF EDITIONS:  2.
        (2)  TOTAL COPY COUNT PER EDITION:  2.
        (3)  CANISTER CONFIGURATION:  16-1-16 (DIGRAPH GF).
   G. (U)  SHIP TO: CA 5A0419 1 CY   CA 159039 1 CY.
   H. (U)  RDD:  24 APR 00
   I. (U)  PURPOSE OF OPERATION:  MATERIAL WILL BE USED FOR GENSER
DIRECT AUTODIN FULL TIME CIRCUIT BETWEEN CDR PIRMASENS AND NCTAMS LANT
NORFOLK VA (CCSD 7D35).
   J. (U)  NET STRUCTURE/OPERATION:  POINT-TO-POINT, FULL-TIME
PIRMASENS CDR TO NORFOLK, VA.  ACTIVATION SCHEDULED NLT 01 AUG 2000.
   K. (U)  SHORT TITLE REPLACED:  NONE.
   L. (U)  KG-84() AUTHORIZED:  CA 5A0419: AUTH 1 OH: 1,
CA 159039: AUTH: 1 OH: 1
   M. (U)  THIS UNIT IS NOT PART OF A COMMAND EMERGENCY REACTION
FORCE.
   N. (C)  KEY USAGE:  TO BE USED BY ACTIVITIES MENTIONED IN SUBPARA 1
ON ITS DAY-TO-DAY MISSION.
2. ALL ADRS WILL BE NOTIFIED BY THE CONAUTH WHEN CRYPTONET IS
IMPLEMENTED.
3. THIS REQUEST HAS BEEN COORDINATED AND APPROVED BY OUR NEXT HHQ,
5TH SIG CMD, ATTN:  ASQK-S.
4.  (U)  POC IS MR. DENNIS HILLIARD, CONAUTH.


P. MICHAUD                                DERIVED FROM:  TB 380-41
CONAUTH, 5932                             DECLASSIFY ON SOURCE MARKED OADR
                                          DATE OF SOURCE:  JUN 03

   DON OWEN, MAJ, CDR
```

**Figure 3-1. Request to Establish a Cryptonet.**

**3.6.1 (U) Requests for Key Tapes.** Some cryptosystems are capable of local key generation (i.e., KY-57, KY-58, and KG-83), in electronic form, for distribution to cryptonet holders without resorting to hard copy key (see NAG 16[XXX]). Local generation of electronic key is the preferred method for operations whether derived from key generation-capable COMSEC equipment, or via the LCMS Workstation. When field generation of key is not a viable option, key must be ordered in hard copy form. Ordering key in tape format requires the commander and COMSEC personnel to be familiar with three different types of key: Traffic Encryption Key (TEK), Key Encryption Key (KEK), and start-up KEK.

**a. (U) Ordering Tape TEK.**

(1) (U) *Uses.* For nets/circuits that distribute TEK via Over-the-Air Re-key (OTAR), tape TEK serves two purposes. At Network Control Stations (NCSs) that derive OTAR TEK from certified KG-83/KGX-93s irregular superseded tape, TEK serves as emergency back up in case of a KG-83/ KGX-93 failure. At NCSs that do not use field-generated TEK, tape TEK is required. Tape OTAR TEK associated with OTAR is not dedicated to any specific net, circuit, or COMSEC equipment. In that application, a short title of appropriately classified key tape can serve as the source of TEK for any or all nets and circuits that are controlled by an NCS.

(2) (U) *Format.* Tape TEK intended for use on nets/circuits that distribute TEK via OTAR is produced in the "V_" format, indicating that each canister contains 62 segments. The second letter of the digraph identifies the cryptoperiod, which may vary with specific applications. See the appropriate KAO to determine approved cryptoperiods.

(3) (U) *Copy Count.* Only one copy is produced of each edition of tape TEK intended for use on nets/circuits that distribute TEK via OTAR, since the using NCS is the only holder. Each alternate NCS should hold its own short title(s) of one-copy tape TEK. *Non-OTAR TEK can have as many copies as the CONAUTH requests*.

(4) (U) *Supersession.* At the discretion of the CONAUTH, tape TEK may be re-supplied on a regular or irregular basis.

(a) (U) *Irregular.* In most tactical applications, the consumption rate for tape TEK is not accurately predictable. For example, a commander who has been designated as a possible NCS for a particular start-up KEK may not serve in that capacity for a long period, or tape TEK held as back up for a stand-alone (non-TRI-TAC) KG-83 may never be used. In applications like this, CONAUTHs should order reasonable quantities of tape TEK. Each edition of this key should be superseded irregularly. If follow-on editions are needed, allow four months for production and delivery. The recommended procurement strategy is to requisition as many editions of a single short title of tape TEK as may be required for each using NCS or alternate NCS. Where tape TEK is held only as back up, the recommended stock level is one month's worth of expected use. That period should be long enough to requisition and obtain a replacement KG-83.

(b) (U) *Regular.* In applications where its use rate can be predicted, the number of 62-segment TEK tape canisters required to meet an NCS's requirement, and the schedule on which they are re-supplied, are inter-related. This requires that the CONAUTH adjust the number of short titles and their supersession schedules to ensure that the required volume of tape TEK is received. For example, if an NCS expects to use 150 segments of tape TEK per month, the CONAUTH should order three monthly-superseded short titles.

**b. (U) Ordering Tape Start-up KEK.**

(1) (U) *Use.* Start-up KEK tape supports the establishment of temporary tactical nets and circuits secured by KY-57, KY-58, KY-67, KYV-5, KY-99A, KY-100, KIV-7, or KG-84A/C equipment. Any commander may order a start-up KEK tape for use by an identified community of potential users. Requestors should allow four months for production and distribution.

(2) (U) *Format.* Start-up KEK tape is produced in the "VA" format (62 segments – daily cryptoperiod).

(3) (U) *Copy Count.* The copy count in which a start-up KEK tape is requisitioned should provide for the expected number of holders and a reasonable number of spare copies to accommodate unplanned additions to the cryptonet. The CONAUTH must designate where spare copies are to be held.

(4) (U) *Supersession.* Each edition of start-up KEK tape is regularly superseded at two-month intervals.

**c. (U) Ordering Tape KEK.** Where physical distribution of keyed fill devices is operationally viable, KEK should be field-generated. However, since many tactical environments require use of tape KEK, guidance for ordering tape KEK is as follows.

(1) (U) *Use.* Tape KEK, rather than tape start-up KEK, should be used on KG-84A/C, KY-57/58/67, and KYV-5/KY-99A/KY-100 secured nets and circuits that exist on a continuing basis and that distribute TEK via OTAR.

(2) (U) *Format.* Tape KEK (except that which is used with KW-46) is produced in the "GF" (16 unique segments – three month cryptoperiod) format. Since only four segments per edition are used each year, the remaining segments are available for cold starts. When a cold start is required, the next segment in the canister will be used. At the end of the quarter, simply pull the next available segment.

(3) (U) *Copy Count.* In point-to-point applications and nets that use a unique KEK for each net member (i.e., nets that OTAR sequentially), the copy count for each edition of tape KEK is two. In nets that OTAR simultaneously, the copy count corresponds to the number of net members. The CONAUTH may order a few extra copies to accommodate possible future cryptonet expansion; however, they must designate where such extra copies will be held.

(4) (U) *Supersession.* Each edition of tape KEK associated with continuing nets and circuits are superseded annually. Tape KEK associated with contingency applications may be requisitioned with irregular supersession, but this places the burden of ensuring continuing resupply on the CONAUTH. In either case, four months should be allowed for production and distribution of tape KEK.

**d. (U) Guidance for Ordering Key Tape.** The following table provides standard recommendations given by system type and digraph (for more information on digraph, see 4.8.1a).

**Table 3-1. Digraph for Systems**

| System | Digraph | Configuration | Cryptoperiod |
|---|---|---|---|
| Fascinator | EB | 5-1-5 | Weekly (7 days) |
| GSP (GUV) | TG | 12-1-12 | Yearly |
| KG-40 | AA | 31-1-31 | Daily (24 Hours) |
| KG-45 | NC | Varies | Varies |
| KG-65/75 | AB | 15-5-75 | Weekly (7 days) |
| KG-66 | LH | 35-1-35 | Varies |
| KG-81/94/194 | VF | 62-1-62 | Three Months |
| | GC | 16-1-16 | Monthly |
| KG-84 | | | |
| OTAR KEK | AF | 31-1-31 | Three Months |
| | GF | 16-1-16 | Three Months |
| OTAR KEK | VA | 62-1-62 | Daily (24 hours) |
| | VB | 62-1-62 | Weekly (7 days) |
| Operational TEK | AA | 31-1-31 | Daily (24 Hours) |
| | GC | 16-1-16 | Monthly |
| | VA | 62-1-62 | Daily (24 hours) |
| | VB | 62-1-62 | Weekly (7 days) |
| KG-95 | GC | 16-1-16 | Monthly |
| KGV-8 | GC | 16-1-16 | Monthly |
| | VA | 62-1-62 | Daily (24 hours) |
| KGV-9 | NC | Varies | Varies |
| KGV-10 (SINCGARS) | ZB | 15-5-75 | Weekly (7 days) |
| KGV-11/15 | NC | Varies | Varies |
| | NE | Varies | Varies |
| KL-43 | AA | 31-1-31 | Daily (24 hours) |
| KY-57/58 (VINSON) | ZB | 15-5-75 | Weekly (7 days) |
| KY-68 | AB | 31-1-31 | Weekly (7 days) |
| | ZB | 15-5-75 | Weekly (7 days) |
| KY-99A/KY-100 | ZB | 15-5-75 | Weekly (7 days) |
| KYV-2 | BB | 5-3-15 | Weekly (7 days) |



FOR OFFICIAL USE ONLY

**3.6.2 (U) AKMS Accounts.** Using the attributes of the LCMS and the communications interfaces provided by the Electronic Key Management System (EKMS), COMSEC accounts could prepare an electronic key order for the generation and distribution of keying material from the Primary Tier 1 Facility (COR) or the Central Facility (CF), as well as generate key locally. Refer to the LMD/KP operator's manual for specific procedures.

**3.6.3 (U) Requests to Hold Other Services' or Agencies' Cryptonets Key.** Commanders who desire to hold key controlled by another Army Command, service, or agency, will forward their requests directly to the CONAUTH for approval. If the CONAUTH is an Army Commander and the request is approved, the CONAUTH will submit the new requirement as directed in subparagraph 3.6.1. If the CONAUTH is non-Army and the request is approved, the CONAUTH will submit the requirement through proper channels to its servicing organization. GPS key does not have a CONAUTH; rather, a Validation Authority approves it. See Appendix B-2, Terms.

**3.6.4 (U) Requests for Foreign Release.** Requests for key that requires release to a foreign government will be forwarded to HQDA as directed in AR 380-40. In addition, a copy of the request will be forwarded to CSLA with an information copy to the NSA (Y271).

## 3.7 CONTROLLING AUTHORITY.

(U) The CONAUTH has responsibility for all communications management functions within a command. The CONAUTH is responsible for supervising and coordinating the collective operational and administrative tasks associated with the management of the cryptonet on behalf of the commander. However, the inherent command responsibility for communications and communications security within an organization rests with the commander and cannot be delegated to any other individual.

**a. (U) Authority.** The CONAUTH should be organizationally senior to cryptonet members, have the staff and expertise to perform essential management functions, and must have the authority to ensure instructions are carried out.

**b. (U) Assignment of CONAUTH Duties.** CONAUTH duties will initially be assigned to the commander of an organization requesting or directing the establishment of the cryptonet. Commanders may designate (in writing) a member of the organization to perform CONAUTH duties on their behalf. For electronically generated key, the organization that directs the key generation performs the CONAUTH functions unless those functions are specifically delegated to another organization in writing.

**c. (U) Transfer of CONAUTH Duties.** The transfer of CONAUTH responsibilities for a particular cryptonet may become necessary (or advantageous) for either administrative or operational reasons. When a transfer of CONAUTH duties occurs, the relinquishing CONAUTH is responsible for notifying the commander, the net members, appropriate key distribution activities, CSLA, and the NSA via message traffic of the change. The gaining CONAUTH must ensure that sufficient operational (and sometimes historical) information is acquired to ensure continuity of net operations.

**d. (U) Contingency Operations.** During the conduct of contingency operations, particularly for nets managed at Echelons Above Corps (EAC), it may be desirable for the CONAUTH to temporarily relinquish operational net control of a particular system to a regional command or net control center in the forward contingency area. This temporary delegation or transfer of operational net control is acceptable; however, it does not relieve the assigned CONAUTH from overall supervisory and management responsibility.

**3.7.1 (U) Management Responsibilities.** The CONAUTH's responsibilities and specific duties are primarily an operational function. However, they include specific logistics support actions, surveillance and oversight responsibilities that must be performed by the CONAUTH in coordination with the operational net manager. The commander should formally designate responsible personnel to perform each of these functions.

**3.7.2 (U) Operational Responsibilities.** The Communications/COMSEC Planning and Management element—traditionally the Staff Signal Officer, Operations Officer, Director of Information Management (DOIM), Installation/Operations/ Maintenance (IOM) Communications and Electronics (C&E), and the State Area Command—perform the operational responsibilities for the National Guard Bureau (NGB). These responsibilities are as follows:

**a. (U) Plan and Identify Requirements.** Routine changes to cryptomaterial requirements should be projected and identified to the supporting distribution facility, CSLA, and the NSA NLT 180 days prior to the operational requirement to ensure production and distribution can be accomplished. Emergency requirements should be requested by the CONAUTH as soon as they are known.

**b. (U) Direct Establishment and Operation of Cryptonet.** The CONAUTH directs the establishment, operation, and management of the material assigned to the cryptonet, as well as designates and maintains a record of cryptonet members and the quantity of key each is authorized to hold. The CONAUTH must know the identity of all cryptonet members and the problems users may be experiencing with the keying material. The CONAUTH must also know the distribution authorities that support the holders of the material and the most expeditious ways of promulgating supersession and other emergency information to all holders of the keying material.

**c. (U) Compromise Control.** The CONAUTH must maintain accurate records on pertinent aspects of the cryptonet in sufficient detail in order to assess the impact of, and to recover from, a compromise. The CONAUTH will ensure all net members are aware of compromises, and that they are in compliance with any recovery actions that have been deemed necessary as a result of the compromise (e.g., extension of cryptoperiod or emergency supersession).

**d. (U) Initiate Recovery/Reconstitution.** The CONAUTH will immediately notify all cryptonet members when a net key is compromised and will determine whether to extend the cryptoperiod of the net key or activate a replacement.

**e. (U) Authorize Key Replacement/ Resupply.** The CONAUTH will authorize key replacement or re-supply in situations where material cannot be supplied in time to meet operational requirements for machine cryptosystems.

(1) (U) The CONAUTH must coordinate with distribution authorities to ensure timely resupply of keying material.

(2) (U) When user accounts have only a two-month supply of key remaining, the CONAUTH must promptly ascertain the status of follow-on material.

(3) (U) If user accounts cannot be re-supplied before remaining key is expended, the CONAUTH must direct users to implement the longest authorized cryptoperiod extension for each remaining key setting (see paragraph 3.7.2g). If the extension is insufficient, or a resupply date cannot be determined, the CONAUTH must report, via message using an IMMEDIATE precedence, to the NSA (Y13) and CSLA so that contingency arrangements can be made. The message must include the short title, the number of net members, a description of the type of operations (e.g., full or part time, fixed or mobile communications center), and an explanation for the cryptoperiod extension.

(4) (U) When time is critical, the CONAUTH may verbally request emergency cryptoperiod extensions from the NSA (Y13) (DSN/STU-III 644-6860 or Commercial [301] 688-6860). When authorization is given verbally, the CONAUTH must take immediate action and not wait for message documentation. Net members must abide by all verbal instructions relayed by the CONAUTH.

(5) (U) For some cryptosystems, the CONAUTH has the authority to shorten the cryptoperiod to enhance security if the cryptonet is unusually large. For example, the cryptoperiod for some cryptosystems used in cryptonets

containing 600 or more holders (copies) may be reduced to 12 hours instead of the standard 24 hours.

**f. (U) Direct Classification Changes.** The CONAUTH will evaluate and approve classification changes for all key (see AR 380-40, paragraph 5-6). Before upgrading key to TS, the CONAUTH must ensure that the material has been previously controlled at the COMSEC account level and has not been issued to a user. For contingency purposes, CSLA must be contacted for a classification change for resupply.

**g. (U) Approve Cryptoperiod Extensions.** The CONAUTH may authorize cryptoperiod extensions up to seven (7) days unless specific systems doctrine limits the extension period. CONAUTHs are not required to report these extensions; however, they must be documented. Additional extension of a cryptoperiod must be approved in advance by the NSA or reported as a COMSEC Incident.

**h. (U) Understand Doctrinal Requirements.** The CONAUTH must understand all doctrinal and operational requirements for missions supported, the proper use of key, and be familiar with the capabilities of the associated equipment or off-line system.

**i. (U) Specify Implementation and Supersession of Key.** The CONAUTH must specify the initial cryptonet activation and key implementation date; designate the contingency editions; inform all cryptonet members, appropriate distribution authorities, and the NSA (Y13) when net key is implemented; and inform the above of the subsequent supersession rate thereafter. *Only the NSA establishes supersession rates!* Except in emergencies, or when key is comprised, the CONAUTH cannot change supersession rates.

**j. (U) Determine Unused Key Status.** The CONAUTH determines if unused key can be placed in contingency status while in secure storage.

**k. (U) Specify Key Change (HJ) Times When Not Prescribed.** The CONAUTH determines and approves the amount of key held at the user level and provides this information to each net member. The CONAUTH will specify HJ time for the cryptonet when the time is not prescribed in the keying material. The time selected for key change must be consistent throughout the cryptonet and chosen to have the least operational impact.

**l. (U) Approve the Issuance of Extracts.** The CONAUTH determines and approves the number of extracts of keying material that may be issued at the user level, except where specified otherwise in the operating instructions of the material, and provides this information to each net member.

**m. (U) Distribution Directions.** The CONAUTH advises the appropriate key distribution authorities, CSLA, and the NSA (Y13) of the COMSEC accounts that will be issued keying material and the number of copies to be issued. For manual cryptosystems (one-time pads, operations codes, authentication systems, etc.), the CONAUTH must first identify specific operational requirements to the NSA (Y271/Y272).

**n. (U) Cryptonet Evaluation.** The CONAUTH must continuously monitor the size, operation, and purpose of the cryptonet. Periodic revalidation that an operational requirement exists is mandatory in conjunction with the Cryptonet Evaluation Report (CER) (see paragraph 3.7.6). The CONAUTH must notify all net members, supporting distribution activities, CSLA, and the NSA (Y13) of any changes in net configuration or keying material status. If manual cryptosystems are concerned, the CONAUTH must notify the NSA (Y27).

**o. (U) Validate Requirements.** The CONAUTH contacts cryptonet members, at least annually, to identify the material they control and to advise each member on how to contact the CONAUTH and all other net members under normal and emergency circumstances. The CONAUTH is authorized to communicate directly with the cryptonet members.

**3.7.3 (U) Logistics Support.** Logistics support responsibilities are directed by the CONAUTH, and it is the COMSEC Custodian who carries out these responsibilities:

**a. (U) Ensure Key Availability/ Sustainment.** Ensure all cryptonet members have sufficient keying material on hand (at least the current edition plus one edition) to sustain the cryptonet.

**b. (U) Generation and Distribution of Electronic Key.** Generate, distribute, and manage locally generated electronic key. Authorize electronic generation, distribution, and physical transfer of key in a common fill device or Data Transfer Device (DTD).

**c. (U) Control of the Reproduction of NSA-Produced Hard Copy Key.** Ensure that reproduced NSA key is kept to the minimum amount essential, properly classified, controlled, and destroyed in the same manner as the original keying material. CONAUTHs, who routinely authorize reproduction of the same material, should increase the copy count of that material.

**d. (U) Ensure Two-Person Integrity (TPI) for TS.** Ensure appropriate two-person integrity procedures are followed for all TS key held until issued/destroyed.

**3.7.4 (U) Key Material Compromises.** Where substantial evidence exists that COMSEC keying material (both locally generated and hard copy) has been compromised, the CONAUTH must take immediate action. Ideally, the CONAUTH will announce precautionary supersession and direct early implementation of uncompromised future material. Emergency supersession of hard copy key must be reported immediately to CSLA and the NSA (Y13) so that resupply action may be taken, replacement material may be produced, and status documents corrected. The CONAUTH will direct traffic reviews of any record traffic encrypted using compromised keying material, when warranted.

**a. (U) Directed Supersession.**

(1) (U) Electronic Key: Superseding electronically generated key can present a unique problem for tactical users. Some of the communications paths used to deliver the key may no longer exist, as some of the relaying units may have redeployed and can no longer serve in that capacity. The CONAUTH must consider the time needed to create or reestablish communications paths before directing supersession.

(2) (U) Hard copy key: The feasibility of superseding hard-copy keying material is contingent on several factors: the number of editions held at the user level; the capacity of the NSA to produce the keying material; and the capability to direct supply replacement. Any decision to supersede must take into consideration the time required to notify all cryptonet members and implement the new material.

**b. (U) Precautionary Supersession.** When precautionary supersession is warranted, but some net members do not hold or cannot be supplied with replacement key via normal logistics channels, several options are available to the CONAUTH. The CONAUTH may (in order of preference):

(1) (U) Electronically generate and distribute replacement key settings or transmit key settings to net members via secure, electrical means. Replacement printed key settings must be encrypted by machine on a one-time pad that has not been compromised and can provide end-to-end encryption equal to the classification of the transmitted key.

(2) (U) Direct the early implementation of uncompromised future editions by those cryptonet members who hold those editions or can be supplied quickly, and exclude from net operations those members who do not hold or cannot be furnished the replacement material.

(3) (U) Physically distribute key to net members in a common fill device or Data Transfer Device (DTD). When keyed, common fill devices and DTDs must be protected at the same level as the key contained therein.

**c. (U) Options.** When supersession is warranted but not feasible, the following options are available to the CONAUTH:

(1) (U) Extend the cryptoperiod of uncompromised keying material up to 24 hours (unless specific cryptosystem doctrine prohibits such extensions or authorizes a longer period).

(2) (U) Suspend cryptonet operations until key can be resupplied.

(3) (U) Continue to use the compromised key. This action would be the **LAST** resort when normal supersession of the compromised material will take place before emergency supersession can be accomplished, when keying material changes have a serious detrimental effect on operations, or when no replacement material is available. The CONAUTH must alert net members by other secure means, if available, that a possible compromise has taken place and direct that users minimize transmissions using the compromised key. Use this option only when continued cryptonet operation is **ABSOLUTELY ESSENTIAL** to the mission.

**3.7.5 (U) Defective Keying Material.** The CONAUTH must report the discovery of defective keying material under their control. The CONAUTH shall direct the retention of the defective material and all associated packaging material pending the receipt of disposition instructions. Reports should be addressed to the NSA (Y13 and Y265), with information provided to CSLA. The NSA (Y13) will provide disposition instructions for defective key and packaging materials by message and, if the material is to be recalled, will provide specific instructions for its return. Recalled keying material must be returned via the Defense Courier Service (DCS); Department of State Courier System; or cleared department, agency, or contractor courier. Transfer reports should state the reason for return, refer to the recall message, and include any other remarks requested in the recall message.

**3.7.6 (U) Key Material Reviews.** AR 380-40 requires all CONAUTHs to review and validate their requirements for the cryptosystems and authentication systems under their control (Cryptosystems Evaluation Report [CER], RCS CSGID-131) per the following criteria:

**a. (U) Annual Reviews.** CSLA will provide the CER to the CONAUTH annually. The CONAUTH will conduct an annual review of keying material used with machine cryptosystems. During the review, the CONAUTH must comply with the following:

(1) (U) Justify any continued use of physical key.

(2) (U) Confirm cryptonet structure, quantities and adequacy of key to meet operational requirements, and a continuing requirement for the key. The cryptonet must be deactivated if no longer needed.

(3) (U) Identify large cryptosystems of low peacetime use that are candidates for placement into contingency status.

**b. (U) Review of Manual Cryptosystems.** The CONAUTH will review all manual cryptosystems annually to:

(1) (U) Validate a continuing requirement for the cryptosystem.

(2) (U) Affirm that the system design and content are adequate and that the status of the material is satisfactory (e.g., operational, contingency, and reserve).

(3) (U) Verify that the present holders of the cryptosystem have a continuing need for the system.

(4) (U) Ensure that no machine or auto-manual system exists which will negate the requirement for the manual system.

**c. (U) Recommendation for Change.** The CONAUTH will recommend changes in keying material content, format, or classification to the NSA (Y13 for machine systems; Y27 for manual systems).

**d. (U) Suspension of Key Material.** CONAUTH response to the annual CER is mandatory. Failure to respond will be reported to the CONAUTHs next higher headquarters and/or MACOM. Continued **FAILURE** to respond to the CER may cause **SUSPENSION** in the distribution of future key material.

**3.7.7 (U) Designating Contingency Keying Material.** When large quantities of cryptomaterials provided for regular consumption are destroyed unused, the CONAUTH should consider placing the material into contingency status. Contingency keying material is cryptomaterial held for future, irregularly occurring requirements in excess of routine operational requirements. The material is not activated until needed for the specific requirement and is not destroyed until after use. Substantial savings in production, distribution, accounting, and destruction are realized when contingency materials are used in place of regularly superseded effective key. Any action to establish a contingency cryptonet must be coordinated with CSLA and the NSA (Y13).

**3.7.8 (U) Disposition Instructions for Keying Material.** The CONAUTH is responsible for issuing disposition instructions to all of their key holders regardless if the instructions were received from CSLA Key Management or were originated by the CONAUTH.

## 3.8 COMSEC KEY.

**3.8.1 (U) Authorization to Receive COMSEC Key.** Authorization to receive COMSEC key or publications is based on the operational and support requirements of each requesting unit or activity. The CONAUTH is the approving authority for establishing the cryptonet and for requisitioning physical key to support the cryptonet when electronic key is not feasible. With the implementation of AKMS/EKMS, electronically generated keying material (ALC-7) will, for the most part, replace physical key. Controlling authorities will delegate key generation to its servicing AKMS COMSEC accounts. CSLA coordinates requests for key, as necessary, to validate the COMSEC account data and production requirements.

**3.8.2 (U) Establishing Cryptonets and Initial Issue of COMSEC Key Material.** Procedures used by units and activities (other than CLSF) for the establishment of cryptonets and the initial issue of COMSEC keying material are presented in paragraph 3.6. The CLSF is also responsible for direct initial issue of material for cryptonets that are totally within the Army and wholly within the CLSF area of responsibility. CSLA, the NSA, and the supporting CLSF will be notified when a newly established current-operational cryptonet (using regularly superseded key) has started operations. This notification allows the automatic resupply of key to begin. CSLA and the NSA will also be notified each time an edition of any contingency key is implemented. This notification ensures the timely resupply of future key.

**3.8.3 (U) Shipment of Physical COMSEC Key.** Initial shipments of physical COMSEC key will originate from the USNDA Central Facility or, in some instances, TYAD (Physical Material Handling System). CSLA will monitor these shipments to ensure the shipments are made on a timely basis.

**3.8.4 (U) Transfer Reports for COMSEC Key.** The Transfer Report (SF 153), which accompanies a key shipment from USNDA, will contain the requisition number for each line item of COMSEC key shipped.

**3.8.5 (U) Excess and Unserviceable COMSEC Key.** Excess and unserviceable COMSEC key will be reported by memorandum or electronic message to CSLA. Reported excess and unserviceable COMSEC key will include short title, edition, and quantity of excess.

**3.8.6 (U) Resupply Procedures for COMSEC Key.**

**a. (U) Regularly Superseded Key.** Regularly superseded key is automatically resupplied based on the supersession rate and distribution schedule established by the CONAUTH. Regularly superseded stock will be shipped to the CLSF from production on a regular basis.

**b. (U) Irregularly Superseded Key**. Irregularly superseded key is resupplied at the request of the CONAUTH.

**c. (U) Resupply of Key.** Requests for resupply of key may be via electronic message or memorandum form, depending on the time element involved. Submit requisitions, as appropriate, to CSLA with an information copy to the NSA, ATTN: COMSEC Account 880099. See Appendix F for POCs and the complete mailing address.

**d. (U) Requisitions for Training and Test Material.** Requisitions for training and test material will be submitted to CSLA by memorandum or message.

**3.8.7 (U) Processing Requests.** When available, initial editions will be issued from general-purpose reserve stocks in the CLSF. CSLA will initiate action to fill all other requests.

**a. (U) Routine Resupply and Redistribution of Keying Material.** All requests for resupply or redistribution of keying material will be submitted by the CONAUTH.

**b. (U) Standard Resupply and Redistribution Request Format.** For standard formats refer to figures 3-2, 3-3, and 3-4.

**c. (U) Availability.** Requests should be sent at the earliest possible date to ensure that follow-on editions are available when needed.

**3.8.8 (U) Classification.** All correspondence pertaining to specific command requirements for classified operational key will be classified, as a minimum, CONFIDENTIAL.

```
                                    ***CONFIDENTIAL***

01  01  081241Z  FEB  03  RR  RR  CCCC        AA  ZYUW   TTC-1
NO
            CDR102NDMIBN FT RILEY KS //5C5598//
            DIRCSLA FT HUACHUCA AZ//SELCL-ID-KEY//
      INFO  DIRNSA FT MEADE MD //Y13//
            SUPPORTING CLSF
C O N F I D E N T I A L
SUBJECT:  USKAK 2121 (U)
A.  (U) TB 380-41 PROCEDURES FOR SAFEGUARDING, ACCOUNTING, AND SUPPLY
CONTROL OF COMSEC MATERIAL.
1.  (C) EDITION ALFA OF USKAK 2121 WILL BE IMPLEMENTED ON 1 JUL 03, WITH
NORMAL SUPERSESSION THEREAFTER.  REQUEST RESUPPLY IAW ESTABLISHED
SUPERSESSION RATE.
2.    (U) POC 2LT HEWITT, CONAUTH, DSN 237-1918
DECLAS OADR









P. MICHAUD                          DERIVED FROM:  TB 380-41
COMSEC CUSTODIAN, 5932              DECLASSIFY ON:  SOURCE MARKED OADR
                                    DATE OF SOURCE:  JUN 03

   DON OWEN, MAJ, CDR

                     ***CONFIDENTIAL***   081241ZFEB03
```

This is an example of a message request for resupply of key. Contents will vary according to local requirements. The supporting CLSF will also be an INFO ADDRESSEE.
**Classified for example purposes only**.

**Figure 3-2. Request for Resupply of Key**

```
                              ***CONFIDENTIAL***

01  01  081241Z  APR  03  RR  RR  CCCC        AA  ZYUW   TTC-1
NO
            CDR102NDMIBN FT RILEY KS //5C5598//
            DIRCSLA FT HUACHUCA AZ//SELCL-ID-KEY//
      INFO  DIRNSA FT MEADE MD //Y13//
            SUPPORTING CLSF
C O N F I D E N T I A L
SUBJECT:  USKAK 1813 (U)
A.  (U) TB 380-41 PROCEDURES FOR SAFEGUARDING, ACCOUNTING, AND SUPPLY
CONTROL OF COMSEC MATERIAL.
1.  (C) DUE TO IMPLEMENTATION OF EDITION XRAY OF USKAK 1813 ON 1 FEB 94
REQUEST RESUPPLY OF ONE EDITION.  USKAK 1813, EDITIONS YANKEE AND ZULU
REMAIN IN CONTINGENCY STATUS.
2.  (U) POC 2LT HEWITT, CONAUTH, DSN 237-1918
DECLAS OADR









P. MICHAUD                          DERIVED FROM:  TB 380-41
COMSEC CUSTODIAN, 5932              DECLASSIFY ON:  SOURCE MARKED OADR
                                    DATE OF SOURCE:  JUN 03

   DON OWEN, MAJ, CDR

                     ***CONFIDENTIAL***   081241ZAPR03
```

This is an example of a message request for resupply of key when key usage changes. Contents will vary according to local requirements. The supporting CLSF will also be an INFO ADDRESSEE.
**Classi fied for example purposes only.**

**Figure 3-3. Request for Resupply of Key when Key Usage Changes**

```
                                    UNCLASSIFIED

01  01  081241Z  APR  03  RR  RR  CCCC        AA  ZYUW   TTC-1
NO
             CDR102NDMIBN FT RILEY KS //5C5598//
             DIRCSLA FT HUACHUCA AZ//SELCL-ID-KEY//
       INFO  DIRNSA FT MEADE MD //Y13//
             SUPPORTING CLSF
UNCLAS   FOUO
SUBJECT:  USKAT 3954 (U)
A. TB 380-41 PROCEDURES FOR SAFEGUARDING, ACCOUNTING, AND SUPPLY
CONTROL OF COMSEC MATERIAL.
1. REQUEST DISTRIBUTION AND COPY COUNT OF USKAT 3954 BE CHANGED EFFECTIVE WITH
EDITION ZULU.  REQUEST USKAT 3954 BE SHIPPED TO ACCOUNTS IN COPY COUND INDICATED.
       COMSEC ACCOUNT      CURRENT       CHANGE        TOTAL
          5C9998              2           +2            4
          5D1212              4           -1            3
          5C9999              2           +1            3
          5E3214              1           +5            6

2. POC CWO L. MORALES, CONAUTH, DSN 237-1918









P. MICHAUD
COMSEC CUSTODIAN, 5932

   DON OWEN, MAJ, CDR

                                         ***UNCLASSIFIED***   081241ZAPR03
```

This is an example of a message request for redistribution of key. Contents will vary according to local requirements. The supporting CLSF will also be an INFO ADDRESSEE.
**Classified for example purposes only.**

**Figure 3-4. Request for Redistribution of Key**

## 3.9 DETERMINING COPY COUNT REQUIREMENTS.

(U) In determining copy count requirements for key, the CONAUTH will consider all of the following:

**a. (U) Security.** The requirement for effective and secure communications.

**b. (U) Administrative Capability.** The organizational capability to administer all elements of the cryptonet and to control the material involved.

**c. (U) Location of Equipment to be Keyed.** Equipment that is located within a short driving or walking distance may be keyed with the same copy of key. Point-to-point systems, which are limited to two holders, may require more than two copies per link or circuit, depending on the configuration of the equipment.

**3.9.1 (U) Excessive Use of Manual and Auto-manual Cryptosystems.** The excessive use of manual and auto-manual cryptosystems may adversely affect the inherent cryptographic security of the system. For example, if the average number and length of messages encrypted daily are unusually high, the copy count of manual and auto-manual cryptosystems may have to be limited. The CONAUTH will establish an acceptable balance between the copy count required for operation and that, which may be excessive for cryptosecurity reasons.

**3.9.2 (U) Rapid Net Expansion.** When Rapid Net Expansion is necessary, the CONAUTH may locally reproduce and control the extra copies. When there is a continuing need for extra copies, the CONAUTH will request a change in copy count.

## 3.10 USER HOLDINGS OF KEY MATERIAL.

(U) Restricting the amount of material on hand is necessary to limit the likelihood and scope of compromises; especially those compromises resulting from subversion, espionage, capture by other forces, or other catastrophe. In addition, resupply and net reactivation can be accomplished more rapidly if extensive future holdings are not involved. This is particularly true in the case of key used by a large number of holders.

**3.10.1 (U) Amount of Key to be Held by COMSEC Accounts.** The amount of key that may normally be held by COMSEC Accounts will be as follows:

**a. (U) Monthly Superseded**. User accounts are authorized to hold at least four editions of all key material but *not to exceed* six months including the current edition.

**b. (U) Other than Monthly Superseded.** Accounts are authorized to have the current effective edition plus five future editions. Resupply procedures, unforeseen changes, and in accounts where the usage rate is more than one edition per month, key usage may necessitate exceeding this level at certain times of the year.

**3.10.2 (U) Number of Holders/Pages Per System.** The number of holders who must originate messages and/or the number of pages per system when using One Time Tapes (OTT), OTPs, and manual codes is limited. Each page of a pad or code and each section of tape may be used **only** one time and then destroyed. Each originator will hold a unique pad, tape or code (or sections of a tape) with which to encrypt. For example, a One Time Code (OTC) such as the Personnel Daily Summary Code, which has 100 pages, could be effectively used among 10 holders for 10 days provided each holder uses only one page per day. Most one-time systems are irregularly superseded and resupply must be ordered by the CONAUTH.

**3.10.3 (U) Joint/Combined Operations.** Joint and/or combined operations requiring intercommunications are projected in contingency plans. Contingency cryptosystems must be obtained and must be in sufficient copy count to support those operations. These cryptosystems will be identified in operation and exercise plans, signal-operating instructions, and related documents necessary to support joint operations.

**3.10.4 (U) Exceptions.** There are exceptional cases wherein units operate in remote areas under extreme conditions and resupply may be

difficult or even impossible. In these cases, authority to hold the required amount of key material beyond the six-month limitation may be obtained through command channels from CSLA. Each approval will be granted on the basis of operational necessity and the resupply situation.

**3.10.5 (U) Amount of Key Issued to Users.** The COMSEC Custodian will only issue that amount of key necessary to satisfy the immediate operational requirement, which is consistent with local resupply capabilities. Protectively packaged keying material will be issued as entire editions, except in those rare situations where operational necessity precludes such issue. Issuing extracts of protectively packaged keying material defeats the purpose of the protective packaging and increases the vulnerability of the key contained therein. Refer to Chapter 4 of this TB for information on key tape canisters.

(U) Key or extracts which are to be carried on special purpose aircraft (for example, airborne command posts) will be limited to the amount of key necessary for the mission. Key carried on special purpose aircraft will be destroyed as soon as possible after supersession, or when its intended purpose has been served, whichever occurs first.

## 3.11 EMERGENCY REQUIREMENTS FOR KEY.

(U) Should on-hand stock of a cryptosystem or authentication system become depleted or compromised, the CONAUTH will request emergency issue of similar undedicated reserve material from the appropriate CLSF. The CLSF will then notify CSLA by electronic message so that immediate resupply action may be taken. Notification will be sent to CSLA with an information copy to the NSA (Y13). See Appendix F for POC addresses listing.

**THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY**

# CHAPTER 4

# ACCOUNTING AND REPORTING PROCEDURES

## 4.1 GENERAL.

**a. (U)** To effectively control the status, disposition and reporting of COMSEC material, it is vital that each COMSEC Custodian, Alternate COMSEC Custodian, and other assigned personnel become familiar with and thoroughly understand accounting and reporting procedures for the COMSEC Material Control System (CMCS), as they apply to traditional accounts and AKMS accounts, respectively.

**b. (U)** Procedures established within this TB and specific requirements contained in the CJCSI 3260.01 publication will be used for accounting and reporting of Positive Control material (PCM).

**c. (U)** AR 710-2, Chapter 2, prescribes the proper administration of unit property books for TOE/TDA units. Army classified COMSEC equipment covered by this TB will be identified in the unit property book. The property book will contain a page for each item of authorized classified COMSEC equipment reflecting authorization and identification data only. Accounting and management data specified in Chapter 4, DA Pam 710-2-1, will not be entered on property book records. Property book pages for classified COMSEC equipment will be annotated as follows: "SEE COMSEC ACCOUNTING RECORD FOR STOCK TRANSACTIONS AND ON-HAND BALANCE."

(1) (U) Basic supply policy and procedures for classified COMSEC equipment and components are contained in AR 710-2 and related procedural pamphlets. Except in those instances where COMSEC is specifically exempted, all material management policies as directed in AR 710-2 will be followed.

(2) (U) COMSEC accounts which do not have a specified supply or maintenance support mission assigned by either Vertical-The Army Authorization Documents System (VTAADS) or General Order, but have been established for the sole purpose of managing organic COMSEC equipment authorized on their VTAADS, are defined as USER ACCOUNTS. User Accounts will use Chapters 1 and 2 of AR 710-2 and DA Pam 710-2-1 as their basic supply guide for managing COMSEC material.

(3) (U) Units and activities managing COMSEC accounts that have been officially assigned a specified supply or maintenance mission in support of organic or non-organic customers are defined in general terms as COMSEC Logistics Support Facilities (CLSFs). Such activities will use Chapters 1, 3, 4, or 5 of AR 710-2 and DA Pam 710-2-2 as their basic supply guide for managing COMSEC material. See Chapter 2 of this TB for a more detailed explanation of COMSEC support activities.

**d. (U)** Policies and Procedures for Property Accountability, AR 735-5, also apply to all COMSEC equipment (also see paragraph 2.9d.).

**e. (U)** Direct communications of routine COMSEC accounting activities are authorized between the COR and those COMSEC accounts reporting to the COR. Address routine COMSEC accounting communications to the COR located at Fort Huachuca, AZ, or Lackland Air Force Base, TX, whichever has been designated to support your COMSEC Account. See Appendix F for a listing of COMSEC POCs.

**f. (U)** There is only one acceptable style and structure of an individual's signature that may be used on the various COMSEC documents, reports, accounting records and forms used in CMCS accounting. Whenever a signature is mandated on any COMSEC document, the official and legally sufficient signature must correspond to and match the actual signature recorded on the individual's government-issued identification card. When this TB refers to an "original signature" it means

the original or a copy, which can be used to verify an individual's signature. A stamped or typed signature is not authorized.

## 4.2 COMSEC MATERIAL ACCOUNTING LEGEND CODES (ALC).

(U) The ALC is a numeric code assigned to COMSEC material to indicate the degree of accounting and control required. The NSA assigns ALC 1, 2, 4, and 6 for NSA-generated electronic key. The generating account assigns ALC 6 and 7 based upon the circumstances under which the material will be used (see Chapter 6). COMSEC material is accountable as follows:

**a. (U) ALC 1.** This material is accountable to the COR by SERIAL NUMBER. For destruction of ALC 1 key material, see paragraph 4.19.

**b. (U) ALC 2.** This material is accountable to the COR by QUANTITY.

**c. (U) ALC 4.** This material is not accountable to the COR; however, the COMSEC Custodian will account for this material locally until final disposition.

**d. (U) ALC 6.** This electronic key is generated by AKMS accounts via the LMD/KP using LCMS software. ALC 6 key is also generated and distributed by the NSA through the EKMS and through the Tier 1. It is reportable and centrally accountable to the COR. The two types of ALC 6 key are Implicit and Explicit Key. The determination is made when the Short Title Assignment Order is submitted by a Controlling Authority (Short Title Assignment Requestor or Ordering Privilege Manager [OPM]). For destruction of ALC 6 key material, see paragraph 4.19.

(1) (U) Implicit Key: Can be distributed at the discretion of the operator at an LCMS Workstation.

(2) (U) Explicit Key: The operator at an LCMS Workstation may distribute Explicit key **only** if there is a valid distribution authorization for that key on the LMD/KP platform. The use of Explicit key by user accounts is **highly discouraged** due to the complexity of the procedures required.

**e. (U) ALC 7.** This electronic key is also generated by AKMS accounts using the LMD/KP and is LOCALLY accountable until final disposition is accomplished. The two types of ALC 7 key are Implicit or Explicit Key. The determination is made when the Short Title Assignment Order is submitted by a Controlling Authority (Short Title Assignment Requester or OPM). Distribution discretion for ALC 7 key is the same as that prescribed for ALC 6 key.

(1) (U) Implicit Key: Can be distributed at the discretion of the operator at an LCMS Workstation.

(2) (U) Explicit Key: The operator at an LCMS Workstation can distribute an Explicit key **only** if there is a valid distribution instruction for that key on the LMD/KP platform. The use of Explicit key is **highly discouraged** due to the complexity of the procedures required.

## 4.3 FILES, FORMS, AND REPORTS.

**a. (U) Files.** COMSEC Custodians must establish and maintain accurate accounting records and files. Instructions for file name, retention, and disposition of Signals Security (SIGSEC) files are found in AR 380-40 and AR 380-40, Appendix C.

**b. (U) Forms.** All entries on manual COMSEC accounting forms will be typewritten or written legibly in black or blue ink. The only exception is hand receipt entries and on-hand balances on Items Register (IR) cards, which will be made in pencil. Table 4-1 contains a list of accounting forms. These forms are available through your pinpoint distribution and/or electronic forms engine (i.e., FormFlow, ProForm, etc.).

**c. (U) Reports.** The Reports Control Symbol (RCS) AMC-877 is required on all manually prepared COMSEC reports submitted to the COR. The RCS will be entered in block 17 of each manually prepared SF 153. All entries on COMSEC accounting reports will be

typewritten or written legibly in black or blue ink. File your reports only after you have properly entered the report on the Control Register (DA Form 4669) and the appropriate Items Register card (DA Form 2011-E or 2011-1-E). Table 4-2 contains a list of accounting reports.

## TABLE 4-1. ACCOUNTING FORMS

| DA FORM | FORM TITLE | GENERAL USE |
|---|---|---|
| **2011-E** | COMSEC Aids Item Register | Used by Traditional COMSEC accounts to record receipt, disposition, and destruction of COMSEC key and publications. |
| **2011-1-E** | COMSEC Equipment Items | Used by Traditional COMSEC accounts to record the status and Items Register final disposition of COMSEC equipment. |
| **2653-E** | COMSEC Account Daily Shift Inventory | Used by facilities to record daily or shift-to-shift inventories. |
| **4669-E** | COMSEC Material Voucher Control Register | Used by all COMSEC accounts to record Voucher (document) Numbers of COMSEC transactions. Start a new register at the beginning of each calendar year. |
| **Standard Form 153** | COMSEC Material Report | Used by all COMSEC accounts to report transfer (T), inventory (I), destruction (D), conversion (I), hand receipt (HR), special possession (SP), and other types of reports. This report is generated through the LCMS Workstation or prepared manually. |

## TABLE 4-2. ACCOUNTING REPORTS

(For ELECTRONIC transactions, refer to Chapter 6 of this TB.)

| REPORT TITLE | GENERAL USE |
|---|---|
| **DA Form 2653-E** | Used by facilities to record daily or shift-to-shift inventories of all classified key and key marked "CRYPTO" to assure continuous protection and control. See paragraph 4.12.3 for instructions on completing this form. |
| **SF 153** | Used for COMSEC material transfer, local inventory (SAIR/CCIR for non-reportable assets), destruction, hand receipt, Conversion Reports, special inventory reports and special possession reports. See paragraph 4.9 for instructions on completing this form. |
| **Change of Custodian Inventory Report (CCIR)** | Used to transfer accountability of the account's assets from one COMSEC Custodian to another. Normally, an outgoing custodian will request a preprinted or ELECTRONIC CCIR from the COR. Exceptions are as follows: (1) In a Traditional COMSEC Account the newly appointed custodian will prepare an SF 153 in cases of sudden and unexpected departures of the custodian and forward to the COR; (2) In an AKMS account, the newly appointed custodian will generate an electronic CCIR in cases of sudden and unexpected departure of the custodian and forward to the COR. For additional information on the sudden and unexpected departure of a custodian refer to Chapter 2, paragraph 2.8. |
| **Semiannual Inventory Report (SAIR)** | The COR preprinted SAIR will be provided to the Traditional COMSEC account for their use in performing an SAIR. The AKMS accounts will generate an SAIR and forward to the COR upon notification from the COR. |
| **COMSEC Account Registration Packet (CARP)** | Used to register or modify EKMS Ids. |

**4.3.1 COMSEC Accounting Reports Guide.**

**a.** (U) Tables 4-3, 4-4, 4-5 and 4-6 are provided as a guide in handling SF 153 transactions. Check the Situation Column and determine which application applies.

**b.** (U) The abbreviation "COR" refers to the Central Office of Record to which the COMSEC account reports.

**c.** (U) Mailing addresses for the two CORs are listed in Appendix F.

# TABLE 4-3. TRANSFER/RECEIPT REPORTS

| Situation | Time of Submission | No. of Copies | Distribution | Remarks |
|---|---|---|---|---|
| Transfer of COMSEC material to an Army Account | At Time of Shipment | 4 | 2 w/Shipment<br>1 COR<br>1 Suspense | Suspense copy is destroyed upon receipt of signed copy |
| Receipt of COMSEC material from an Army Account | Within 2 workdays of receipt (TYAD – 10 workdays after receipt) | 2 | 1 Shipper<br>1 File | |
| Transfer of COMSEC material to another service or agency | At time of shipment | 7 | 5 w/Shipment<br>1 COR<br>1 Suspense | Advance copy is sent to the COR |
| Receipt of COMSEC material from another service or agency | Within 2 workdays of receipt | 5 | 5 Shipper<br>1 COR | If shipper is NSA 870___ or from 880___, return two copies directly to the NSA |
| Receipt of COMSEC material without accompanying Transfer Report | Within 2 workdays of receipt | 3 | 1 COR<br>1 Shipper<br>1 File | Indicate Below NOTHING FOLLOWS circumstances including package number and date of receipt |
| Receipt of COMSEC material from non-DoD activities | Within 2 workdays of receipt | 4 | 2 Shipper<br>1 COR<br>1 File | |

TABLE 4-4. DESTRUCTION REPORTS

(For ELECTRONIC transactions, refer to Chapter 6 of this TB.)

| Situation | Time of Submission | Copies | Distribution | Remarks |
|---|---|---|---|---|
| Routine destruction of COMSEC Material (SF 153) | Within 5 days of reporting period | 2 | 1 COR<br>1 File | TYAD and CLSF accounts are authorized additional 10 days |
| Destruction of compromised COMSEC material (SF 153) | Within 5 days of destruction | 2 | 1 COR<br>1 File | |
| Emergency destruction of COMSEC material (SF 153) | Immediately after destruction | 2 | 1 COR<br>1 File | Indicate EMERGENCY DESTRUCTION in Remarks column |



FOR OFFICIAL USE ONLY

# TABLE 4-5. INVENTORY REPORT (TRADITIONAL ACCOUNTS)

| Situation | Time Of Submission | Copies | Distribution | Remarks |
|---|---|---|---|---|
| Preprinted Semiannual Inventory (SAIR) | C&C page returned within 45 days of "date of report" on the preprinted report. | 2 | 1 COR<br>1 File | ARNG/USAR accounts are authorized additional 15 days |
| Printed Change of Custodian Report | C&C page is returned immediately, but NTE 60 days. | 2 | 1 COR<br>1 File | Voided by COR 45 days from date of report. |
| Special Inventory – Manual Change of Custodian Report (SF 153) | Immediately after inventory | 2 | 1 COR<br>1 File | Upon sudden and unexplained departure of the custodian. |
| Special Inventory – Movement or Deployment of a unit to another geographic area (SF 153) | Immediately prior to departure and after arrival at destination | 1 | 1 File | |
| Conversion Report (SF 153) | Immediately after adjustment | 2 | 1 COR<br>1 File | Used to report change of short title and/or serial number of material or equipment / component conversion from one configuration to another. |
| Special Possession Report-COMSEC material recovered after being lost and removed from accountability | Immediately after recovery | 2 | 1 COR<br>1 File | Indicate circumstances involved. |
| Special Possession Report–COMSEC material found which is not on accounting records (SF 153) | Immediately after discovery | 2 | 1 COR<br>1 File | Indicate circumstances involved |

# 4.4 RECEIPT INSPECTION AND INVENTORY OF COMSEC MATERIAL.

**4.4.1 (U) General.**

**a. (U)** In addition to routine distribution and normal receipt of requested material, COMSEC material may be received from multiple sources for a variety of reasons, such as the recovery of lost or stolen material, conversion of existing equipment, updating of theater COMSEC equipment, etc.

**b. (U)** All packages, containers, keying material and publications must be examined to determine if outer wrappings have been tampered with and carefully opened to examine inner contents.

**c. (U)** The using activity custodian will open equipment containers within 2 working days after receipt. EXCEPTION: This does not apply to current or future FORTEZZA cards (KOV-13 and KOV-14 cards are considered equipment) still in their sealed, transparent, protective containers.

**d. (U)** CLSFs are exempt from the requirement to open sealed containers when the containers are only being handled for further distribution IAW paragraph 4.4.7b.

**4.4.2 (U) TOP SECRET Key.** TOP SECRET key received sealed in its protective packaging does not require Two Person Integrity (TPI) controls as long as the key is in the possession of the COMSEC Custodian, and that custodian is in the DA Cryptographic Access Program (DACAP).

**a. (U)** When the protective packaging is opened within the account and when the material is hand-receipted to a user, all TOP SECRET material will be signed for by two individuals and maintained under TPI controls.

**b. (U)** Additional information on the control and storage of TOP SECRET key, the application of TPI controls, and the use of No-Lone-Zones is contained in Chapter 2, AR 380-40.

**4.4.3 (U) Package/Container Examination.** The COMSEC Custodian or the alternate will physically examine all incoming packages and containers.

**a. (U) Inspection.** Check for evidence of attempts to open or alter the package. Verify that the contents of the package have not been exposed. If the package or container has been tampered with or the contents exposed, perform the following:

(1) (U) Photograph the package in its actual condition immediately upon receipt.

(2) (U) Submit an incident report as directed in Chapter 7.

(3) (U) Do not open the package or container until authorized by the NSA.

**b. (U) Improperly Delivered Package.** If a package has been improperly delivered to an individual other than the COMSEC Custodian, Alternate COMSEC Custodian or an individual listed on DCS Form 10 and then delivered to the custodian unopened and untampered with, the package will be opened and the contents verified against the enclosed Transfer Report.

**c. (U) Verification of Contents.** The COMSEC Custodian or the alternate will check all packages and containers for:

(1) (U) *Short title(s).*

(2) (U) *Serial/register number(s).*

(3) (U) *Quantity.*

**d. (U) Discrepancies.** Any discrepancy must be reported to both the shipping COMSEC Custodian and the COR. After checking the shipment and reporting any incident, if required, correct the Transfer Report to agree with the shipment.

**4.4.4 (U) Transfer Reports SF 153.** The receiving COMSEC Custodian will sign and dispatch the Transfer Report to the shipping COMSEC Custodian within 2 working days of receipt of the shipment. After acknowledging receipt of the COMSEC material, enter the received material onto the LCMS Workstation or

on the appropriate Items Register Card(s). A copy of all vouchers received from non-Army accounts will be sent to the COR.

**4.4.5 (U) Page-Checking Keying Material.** The individual user must verify or have verified the presence of each page of unsealed "CRYPTO"-marked keypads and lists upon receipt, transfer, SAIR, Change of Custodian, and before destruction. CLSFs holding key for further distribution are exempted from page-checking requirements. A record of page checking (name, grade, unit, and date) will be posted to the Record of Page Check or the first page of the document.

**a. (U) Missing Pages.** When a page is discovered missing, submit an incident report as directed in Chapter 7 of this TB.

**b. (U) Duplicate or Misnumbered Pages.** If duplicate or misnumbered pages are received, submit a report classified CONFIDENTIAL to the CONAUTH with an information copy to COR and the NSA (see Appendix F for addresses). No further reporting is necessary unless directed. In case of duplicate pages, destroy the excess pages and prepare a Local Destruction Report.

**c. (U) Extracts.** A keypad with extracts removed is considered partially destroyed. However, any keypad with extracted pages will be page-checked prior to destruction to ensure that all extracted material has been destroyed.

**4.4.6 (U) Page-Checking COMSEC Publications (KAM, KAO, etc.).** Upon receiving COMSEC publications, conduct an initial, page-by-page inventory to verify that each page is present and in proper order for both instructional- and general-type publications. A record of page checking will be posted to the Record of Page Check of accountable documents. CLSFs holding accountable COMSEC publications for further distribution are exempt from page checking. Additional page checks *must* also be performed:

- (U) After posting amendments, which may affect page numbers or contain replacement pages.
- (U) Prior to document destruction.
- (U) Upon change of custodian.
- (U) When publication is transferred.
- (U) Annually within 1 year after the last page check.

(U) If, when page-checking accountable COMSEC publications, you find:

**a. (U) Missing Pages During Initial Check:** Submit a report classified according to contents to the office that issued the publication. Always note the circumstances and the material involved. Take no further action unless directed by the issuing office.

**b. (U) Missing Pages After the Initial Check:** Prepare and submit a COMSEC Incident Report IAW paragraph 7.5 and AR 380-40. This report will be classified IAW AR 380-40. Include the issuing or shipping account as an addressee.

**c. (U) Duplicate Pages:** Submit a report classified according to contents to the NSA, ATTN: Y13 (see Appendix F). No further reporting is necessary unless directed. The duplicate pages will be destroyed and a Local Destruction Report prepared.

**4.4.7 (U) Inventory of Sealed Material, Packages, and Shipping Containers.**

**a. (U)** For purposes of security and preservation of contents, it is necessary that many accountable COMSEC material items be sealed when manufactured. These items are not to be opened unless the material is to be used within 72 hours or a physical security check is to be conducted due to package tampering.

**b. (U)** For efficient use of material and labor, certain packages and containers are unit-packed (i.e., multiple related items within a single package). In these cases, the intent is to distribute these fixed quantities to the lowest level user without the need for opening or repackaging. When checking or inventorying COMSEC material in sealed packages proceed as follows.

(1) (U) Unit-Packed Keying Material.

(a) (U) Unit-packed COMSEC material such as key tapes and keypads will not be opened at intermediate storage and shipping points, such as a CLSF. When the CLSF needs to

check or inventory these items, verify the following information from the external packaging label:

- (U) Short Title
- (U) Edition
- (U) Quantity
- (U) Serial/Register Number

(b) (U) CLSFs may receive packages containing key tapes and other similar material. The CLSF may open these packages for partial distribution. If opened, the CLSF will reseal these packages as follows:

- (U) Re-tape the packages.
- (U) Correct the label to reflect the remaining short title/edition, quantity, and serial/registration numbers.

(c) (U) Packages of unit-packed material opened by CLSFs are subject to normal inventory procedures (SAIR, CCIR) until repacked and sealed.

(2) (U) Key Tape Plastic Canister.

(a) (U) The tape is divided into key segments with all segments containing the short title/edition, the serial/register number, and the key tape segment number. Depending on the ALC, the key tape canister will be hand-receipted or issued to individual users in its entirety. Individual key tape segments can be issued IAW the CONAUTHs instructions (see Chapter 3 of this TB).

(b) (U) Upon receipt, if the short title does not appear in the canister window, tampering has occurred and an incident report must be submitted. Do not remove key tape segments for inventory.

(c) (U) Inventory the tape canister by comparing the disposition record card with the tape segment appearing in the canister window. When a discrepancy is discovered, an incident report must be submitted. Retain the completed disposition record: after the empty tape canister is destroyed, attach the record to the file copy of the destruction voucher.

(3) (U) Pads Sealed by Gum Adhesive.

(a) (U) Material such as one-time pads sealed by gum adhesive may be received by a limited number of users. Do not open these items prior to issue to the user. Even when opened, the gum adhesive is considered adequate verification of the presence of unused pages. To check or inventory such items, obtain the following information from the cover:

- (U) Short Title/Edition
- (U) Serial/Register Number

(b) (U) There may be rare cases when partially used one-time pads are transferred between COMSEC accounts. In such cases, the Transfer Report will bear a notation indicating which pages have been used (e.g., “KAP AA 27 less pages 1 through 49”). The local destruction certification showing the destruction of the used pages will accompany the partially used key. The shipping custodian will retain a copy of the local destruction certificate in the COMSEC account files.

## 4.5 ASSIGNMENT OF COMSEC MATERIAL VOUCHER NUMBERS.

**a. (U) AKMS Account Voucher Numbers.** COMSEC Material Voucher Numbers for AKMS Accounts will be automatically assigned by the system.

NUMBERS ARE SEQUENTIAL. THERE IS NO SEPARATION OF ACCOUNTABLE AND NON-ACCOUNTABLE NUMBERS.

**b. (U) Traditional Account Voucher Numbers**. For traditional (manual) accounts, the custodian will assign voucher numbers to COMSEC Material Reports. A voucher number consists of the COMSEC account number, Julian date of the report, and a sequential outgoing voucher number (see paragraph 4.6).

**(1) (U) Reportable outgoing COMSEC Material voucher numbers.** Voucher number series (0001-4999) will be assigned to transactions that are to be reported to the COR.

(a) (U) If a duplicate or out-of-sequence voucher number is erroneously used, a correction must be sent to the COR.

(b) (U) If an outgoing voucher number is skipped, inform the COR of the error and state that the number is marked VOID on the COMSEC Material voucher control register. A voided voucher number will not be used again during the same calendar year.

(c) (U) At the beginning of each calendar year, upon submission of the first voucher to the COR, list the last outgoing voucher number used during the previous year (e.g., below the "NOTHING FOLLOWS" entry on the SF 153, annotate, for example, "Last outgoing voucher number used during 1999: 5D5570-9331-0128").

**(2) (U) Local COMSEC Material Voucher Numbers.** Outgoing voucher numbers (5000-9999) are assigned to local transactions that are not forwarded to the COR. Examples of local COMSEC reports are as follows:

- (U) Transfer of ALC 4 material
- (U) Hand Receipts
- (U) Local Destruction Reports
- (U) Issue of ALC 4 material
- (U) Receipt (transfer-ins) optional
- (U) Inventory of selected ALC 4 material (only when an SF 153 is used)
- (U) Locally reproduced material

**(3) (U) EXCEPTION:** When a COMSEC Custodian originates an SF 153 Change of Custodian Inventory Report (CCIR), or Special Inventory Report to the COR, a voucher number will **NOT** be assigned. Instead, the custodian will enter the Julian date in block 4 of the SF 153 followed by the designation "CUST."

**(4) (U) Other Service Voucher Numbers.** COMSEC material shipped to Army COMSEC accounts from other services is shipped under the other service's voucher. This number cannot be processed through the Army CMCS unless it has been modified as shown in Table 4-6. When changing another service's voucher number, only the last five digits in block 4 of the SF 153 will be modified (see the following conversion chart).

Table 4-6. Modification of Other Services' Voucher Numbers

| Shipper | SF 153 From | SF 153 Block 3 | SF 153 Block 4 | After Conversion (This entry goes on IR Card) |
|---|---|---|---|---|
| NSA | 880099 | 99 11 21 | 58086 | 880099-9325-58086 |
| CF | 880103 | 99 11 21 | 13576 | 880103-9325-13576 |
| AF | 616600 | 99 11 21 | 92550030 | 616600-9325-50030 |
| NAVY | 241120 | 99 11 21 | 230041 | 241120-9325-30041 |
| AKMS AC | 5AT152 | 19990609 | 00036 | 5AT152-9160-00036 |

**Change calendar date to Julian date**

## 4.6 PREPARATION OF VOUCHER CONTROL REGISTER (DA FORM 4669-E) (NOT APPLICABLE TO AKMS).

**4.6.1 (U) Use of DA Form 4669-E.** COMSEC Material Voucher Control Registers are used to maintain a record of transaction voucher numbers. Each recorded voucher number represents an account transaction (i.e., Transfer Report, Destruction Report, hand receipt, etc.). Two registers must be maintained: one to record outgoing transactions accountable to the COR (0001-4999), and one recording local transactions (5000-9999). Use of these registers will ensure that a voucher number is not duplicated. If the full range of voucher numbers is used prior to year-end, start over with 0001 or 5000, as appropriate. New registers must be started at the beginning of each calendar year.

**4.6.2 (U) DA Form 4669-E Completion Instructions** (see Figures 4-1 and 4-2).

**a. (U) Block 1, Account Number.** Enter the assigned COMSEC account number.

**b. (U) Block 2, Dates.** Enter in the FROM block the date (DAY/MONTH/YEAR) the Voucher Control Register page is started. When both sides of the form are completed, or at the end of the year, enter the ending date in the TO block.

**c. (U) Block 3, Organization/Activity.** Enter the name of your organization or activity and the word OUTGOING or LOCAL depending upon the type of register.

**d. (U) Block 4, Unit Identification Code.** Enter the UIC of the preparing organization or activity.

**e. (U) Block 5, Page Number.** Each form will be identified as a single page. Begin with number 1 and then additional forms, if needed, will be sequentially page numbered throughout the calendar year.

**f. (U) Block 6, Voucher Number.** Enter the Julian date and assigned OUTGOING or LOCAL transaction number.

**g. (U) Block 7, To.** Enter the account number of the receiving account or individual's name (as applicable). In the case of a hand receipt, enter the name of the individual holding or receiving the material.

**h. (U) Block 8, DCS Register Number.** Enter the DCS voucher number or registered mail number, if applicable.

**i. (U) Block 9, Transaction Description.** Enter a description of the transaction.

**j. (U) Block 10, Remarks.** Enter the initials of the individual making the control register entry indicating that all necessary actions have been completed.

| COMSEC MATERIAL VOUCHER CONTROL REGISTER<br>For use of this form, see TB 380-41; the proponent agency is AMC | 1. ACCOUNT NUMBER<br>5C7092 | 2. DATES (Day month year)<br>a. FROM 1 JAN 03 | b. TO |
|---|---|---|---|
| 3. ORGANIZATION/ACTIVITY OUTGOING<br>88th FLD Arty Bde | | 4. UIC<br>WHAACR | 5. PAGE:<br>1 |

| 6. VOUCHER NUMBER | 7. TO | 8. DCS REGISTERED NUMBER | 9. TYPE TRANSACTION | 10. REMARKS |
|---|---|---|---|---|
| 3010-0001 | 5SN000 | | Consolidated Destruction Report | GBC |
| 3020-0002 | 5D2987 | BZ6126 | Transfer Out | JC |
| 3036-0003 | 5SN000 | | Consolidated Destruction Report | HG |
| 3057-0004 | 5SN000 | | Special Possession Report | GBC |
| 0005 | | | VOID | Erroneously assigned to local voucher. COR notified 3 Mar 00 |
| 3062-0006 | 5SN000 | | Consolidated Destruction Report | HG |
| 3091-0007 | 5D3001 | BZ2626 | Transfer Out | HG |
| | | | | |
| | | | | |

DA FORM 4669-E, JUL 03

**Figure 4-1. COMSEC Material Voucher Control Register (Outgoing)**
**(DA Form 4669-E)**

| COMSEC MATERIAL VOUCHER CONTROL REGISTER<br>For use of this form, see TB 380-41; the proponent agency is AMC | 1. ACCOUNT NUMBER<br>5C7092 | 2. DATES (Day month year)<br>a. FROM 1 JAN 03 | b. TO |
|---|---|---|---|
| 3. ORGANIZATION/ACTIVITY LOCAL<br>88th FLD Arty Bde | | 4. UIC<br>WHAACR | 5. PAGE: |

| 6. VOUCHER NUMBER | 7. TO | 8. DCS REGISTERED NUMBER | 9. TYPE TRANSACTION | 10. REMARKS |
|---|---|---|---|---|
| 3002-5000 | CPT Moore | | Hand Receipt | HG Mat returned 16 Jan 93 |
| 3009-5001 | | | Local Destruction Report | GBC |
| 3035-5002 | | | Local Destruction Report | HG |
| 3061-5003 | | | Local Destruction Report | GBC |
| 3061-5004 | SSG Gold | | Hand Receipt | KLG |
| | | | | |
| | | | | |

DA FORM 4669-E, JUL 03

(U) When material is returned, draw one line through the entry in the LOCAL Register and annotate: "Material returned" plus date of return and your initials in the Remarks Column. This applies to hand receipts only.

**Figure 4-2. COMSEC Material Voucher Control Register (Local)**
**(DA Form 4669-E)**

## 4.7 ITEM REGISTER (IR) CARDS (NOT APPLICABLE TO AKMS).

**4.7.1 (U) General Instructions.** *AKMS accounts are not required to maintain IR Cards.*

**a. (U)** The following IR Cards will be used:

(1) (U) DA Form 2011-E, COMSEC Aids Items Register.

(2) (U) DA Form 2011-1-E, COMSEC Equipment Items Register.

**b. (U)** IR Cards will be maintained for all ALC 1, 2 and 4 material from time of receipt to final disposition.

**c. (U)** Single editions of COMSEC material per IR Card may be used by accounts when the COMSEC Custodian considers this accounting method to be an advantage in managing his/her account. Single-line entries should be used for equipment entries to facilitate hand receipting and transfers. Correction fluid (white-out) can be used to make corrections to IR Cards.

**d. (U)** Although hand receipts for TOP SECRET (TS) material require two signatures, the Disposition block on the Item Register Card only requires the name of the primary Hand Receipt Holder. The primary Hand Receipt Holder is the person signing in block 15a of the SF 153.

**e. (U)** Special Possession and Conversion Report voucher numbers will be recorded in the receipt portion of the IR Cards to show the source from which the material was received or modified. In addition, Conversion Report voucher numbers will also be recorded in the disposition portion of the IR Card to show why certain material is no longer in the account.

**4.7.2 (U) DA Form 2011-E COMSEC Aids Items Register.**

**a. (U) DA Form 2011-E.** DA Form 2011-E is used by all manual COMSEC accounts to record receipts, hand receipts, issues, transfers, special possessions, and destructions. This form may be used as a destruction certificate when signed by the COMSEC Custodian or alternate COMSEC Custodian and a witness. It may also be used for issuing ALC 4 material by having the user sign and print his/her name in the destruction portion of the IR Card. A separate DA Form 2011-E will be maintained for each short title of COMSEC key and publications held by a COMSEC account. It is recommended that when an account receives multiple copies of each edition of a short title, separate IR Cards be prepared for each edition. The use of separate IR Cards will facilitate orderly accounting of material COMSEC aids and provide a clear audit trail. Figures 4-3 and 4-4 show two methods of recording destruction. Any combination of these may be used. Record information as is directed in the following paragraph.

**b. (U) DA Form 2011-E Completion Instructions** (see Figures 4-3 and 4-4).

(1) (U) *SHORT TITLE*. Enter the short title for the COMSEC material represented.

(2) (U) *NSN/MCN*. Enter the NSN/MCN for the material (this entry is optional).

(3) (U) *LOCATION*. Enter the physical location of material represented (this entry is optional).

(4) (U) *ALC*. Enter the ALC for material represented.

(5) (U) *ACCOUNT NO*. Enter the COMSEC account number.

(6) (U) *EDIT/REG*. Enter the edition designator or register number for the entry.

(7) (U) *SERIAL NUMBERS*. Enter serial numbers as follows:

(a) (U) Use one line for a consecutive series of serial numbers with the beginning serial number in the BEGIN column and the ending serial number in the END column. In some cases, single-line entries for a series of serial numbers provide a better control of the material being used.

(b) (U) If one serial number per line is used, enter that serial number in the END column.

(c) (U) For ALC 2 material, enter the quantity (e.g., 1 ea, 2 ea) instead of the serial number.

(8) (U) *RECEIPT*:

(a) (U) FROM. Enter account number of the shipper from block 2 of the incoming SF 153.

(b) (U) DATE. Enter the Julian date from block 4 of the incoming SF 153.

(c) (U) SERIAL. Enter the shipper's outgoing voucher serial number from block 4 of the incoming SF 153.

(9) (U) *DISPOSITION*.

(a) (U) TO. Enter the appropriate code to indicate the type of transaction:

C – Conversion
CD – Consolidated Destruction
D – Destruction
HR – Hand Receipt
I – Issue
SP – Special Possession.
T – Transfer

(U) For a transfer, record the account number of the receiving COMSEC account. For hand receipts and issues (ALC 4), enter the name of the receiving individual (use pencil for hand receipts).

(b) (U) DATE/SERIAL. Enter the Julian date of the transaction. Enter the voucher serial number below the date.

(10) (U) *DEST/ISSUED DATE.* Enter the Julian date of local destruction or issue of ALC 4 material.

(11) (U) *DESTRUCTION CERTIFICATIONS (OPTIONAL)*. This column may be used for signatures of the COMSEC Custodian and a witness to certify the destruction of COMSEC material. The signature of the custodian and a witness in this column certifies that these two individuals personally destroyed the material. This procedure eliminates the requirement for individual Local Destruction Reports. At the end of each month, a Consolidated Destruction Report will be submitted to the COR listing all reportable material from the Items Register Cards that have not been previously reported. When the Items Register Card is used for the issue of ALC 4 material, the recipient will sign block 1 and print his/her name and rank in block 2.

**COMSEC AIDS ITEMS REGISTER** *(USING Unit)* For use of this form, see TB 360-41; the proponent agency is AMC

| SHORT TITLE | NSN/MCN | LOCATION | ALC | ACCOUNT NO |
|---|---|---|---|---|
| USKAK 9717 | 581000U309091 | Safe 18 | 1 | 5DE180 |

| EDIT/ REG | SERIAL NUMBERS BEGIN | SERIAL NUMBERS END | RECEIPT FROM | RECEIPT DATE / SERIAL | DISPOSITION TO | DISPOSITION DATE / SERIAL | DEST/ ISSUE DATE | DESTRUCTION CERTIFICATION 1. CUSTODIAN | DESTRUCTION CERTIFICATION 2. WITNESS |
|---|---|---|---|---|---|---|---|---|---|
| AE | | 107 | 880099 | 0079 | (D) | 0155 | | 1 | |
| | | | | 0021 | | 0020 | | 2 | |
| AE | | 108 | 880099 | 0079 | | 0160 | D 0157 | 1 Don Quinnetter | |
| | | | | 0021 | (CD) | 0032 | | 2 Pamela Defer | |
| AE | | 109 | 880099 | 0079 | | 0160 | D 0158 | 1 Don Quinnetter | |
| | | | | 0021 | (CD) | 0032 | | 2 Larry Bryson | |
| AE | | 340 | 5CE078 | 0090 | (T) 5DE927 | 0095 | | 1 | |
| | | | | 0134 | | 0029 | | 2 | |
| AE | | 101 | 5CE078 | 3090 | | | | 1 | |
| | | | | 0148 | | | | 2 | |
| | | | | | | | | 1 | |
| | | | | | | | | 2 | |
| | | | | | | | | 1 | |
| | | | | | | | | 2 | |
| | | | | | | | | 1 | |
| | | | | | | | | 2 | |
| | | | | | | | | 1 | |
| | | | | | | | | 2 | |
| | | | | | | | | 1 | |
| | | | | | | | | 2 | |

DA FORM 2011-E
1 JUL 03

THIS FORM, TOGETHER WITH DA FORM 2011-1-E, 1 JUL 03
REPLACES DA FORM 2011-1, 1 NOV 77, WHICH IS OBSOLETE

(U) All hand receipt information must be entered in pencil and erased when the material is returned. The “0157/0158” entry in the Dest/Issue Date Column reflects the actual date of destruction. The IR Card must be signed certifying destruction at the same time the destruction date is entered.

**Figure 4-3. COMSEC Aid Items Register (ALC 1 Material)**

COMSEC AIDS ITEMS REGISTER *(USING Unit)*

For use of this form, see TB 380-41; the proponent agency is AMC

| SHORT TITLE | NSN/MCN | LOCATION | ALC | ACCOUNT NO |
|---|---|---|---|---|
| USKAK 1430 | (Optional) | (Optional) | 4 | 5DE234 |

| EDIT/ REG | SERIAL NUMBERS BEGIN | SERIAL NUMBERS END | RECEIPT FROM | RECEIPT DATE / SERIAL | DISPOSITION TO | DISPOSITION DATE / SERIAL | DEST/ ISSUE DATE | DESTRUCTION CERTIFICATION 1. CUSTODIAN 2. WITNESS |
|---|---|---|---|---|---|---|---|---|
| W | 8 | 28 | 5BE001 | 3285<br>3214 | | | | 1<br>2 |
| W | | 8 | | | (I) SSG WEBB | 3332<br>5352 | | 1<br>2 |
| W | 9 | 10 | | | | | (I) 3332 | 1 Bill Cole<br>2 CW2 Bill Cole |
| W | 11 | 17 | | | | | (I) 3333 | 1 Ira Levin<br>2 SSG Ira Levin |
| W | | 18 | | | (I) LT Brown | 3332<br>5352 | | 1<br>2 |
| W | 19 | 20 | | | (T) 5DE422 | 3301<br>5342 | | 1<br>2 |
| W | | 21 | | | | | (D) 3323 | 1 Levin Jones<br>2 Thomas Hall |
| W | 22 | 28 | | | (D) | 3323<br>5001 | | 1<br>2 |
| | | | | | | | | 1<br>2 |
| | | | | | | | | 1<br>2 |

DA FORM 2011-E
1 JUI 03

THIS FORM, TOGETHER WITH DA FORM 2011-1-E, 1 JUL 03
REPLACES DA FORM 2011-1, 1 NOV 77, WHICH IS OBSOLETE

**Figure 4-4. COMSEC Aids Items Register (ALC 4 Material)**

**4.7.3 (U) DA Form 2011-1-E COMSEC Equipment Items Register.**

**a. (U) DA Form 2011-1-E.** DA Form 2011-1-E is used by all **traditional** accounts to record receipts, transfers, hand receipts, conversions and loan transactions. Unlike DA Form 2011-E, the 2011-1 cannot be used as a destruction certificate. A separate DA Form 2011-1-E will be maintained for each COMSEC equipment short title held by a COMSEC account. When completing Items Register Cards, it is encouraged to annotate (I) for Issue, (T) for Transfer, (D) for Destruction, and (H/R) for Hand Receipt, where applicable.

**b. (U) DA Form 2011-1-E.** Completion Instructions (see Figures 4-5 and 4-6):

(1) (U) *SHORT TITLE.* Enter the short title for the COMSEC material represented.

(2) (U) *NSN/MCN*. Enter the NSN/MCN for the material (this entry is optional).

(3) (U) *END ITEM.* Enter the short title for the end item involved. If the item is an end item, for example a KG-31B, no entry will be made in this block.

(4) (U) *ALC.* Enter the ALC number for material represented.

(5) (U) *ACCOUNT NO.* Enter the COMSEC account number.

(6) (U) *QTY.* Enter the quantity for all material that is accountable by quantity. This entry is optional for ALC 1 items.

(7) (U) *SERIAL NUMBERS.* Enter serial numbers as follows:

(a) (U) Enter serial numbers for ALC 1 items.

(b) (U) If one serial number is used per line, enter that serial number in the END column. In some cases, single-line entries for a series of serial numbers provide a better control of the material being used.

(c) (U) Serial number entries are optional for material accountable by quantity.

(8) (U) *RECEIPT.*

(a) (U) ACCOUNT. Enter account number of the shipper from block 2 of the incoming SF 153.

(b) (U) DATE. Enter the Julian date from block 4 of the incoming SF 153.

(c) (U) SERIAL NUMBER. Enter the shipper's outgoing voucher number from block 4 of the incoming SF 153.

(9) *(U) TRANSFER.*

(a) (U) ACCOUNT. Enter the account number of the recipient from block 7 of the outgoing SF 153. For hand receipts, enter the Hand Receipt Holder's rank and last name under the letters HR in pencil.

(b) (U) DATE. Enter the Julian date from block 4 of the outgoing SF 153. For hand receipts, enter the Julian date in pencil.

(c) (U) SERIAL NUMBER. Enter the outgoing voucher serial number from block 4 of outgoing SF 153.

(10) *(U) LOAN DATA.*

(a) (U) FROM. Enter the service or agency borrowing the equipment.

(b) (U) DURATION. Enter the number of days the equipment is out on loan, normally 12 months or less (see AR 700-131).

(11) (U) *ON-HAND BALANCE*. Enter the total on-hand balance with each entry. The balance will include material on hand receipt for which the COMSEC Custodian retains accountability. This entry is not required for items the custodian is maintaining serial number accountability. On-hand balances should be annotated in pencil to allow changes.

| **COMSEC EQUIPMENT ITEMS REGISTER** *(USING UNIT)* | | | | | | | | | | | For use of this form, see TB 360-41; the proponent agency is AMC |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SHORT TITLE<br>HY 4112 | | | | NSN/MCN<br>558100101700084 | | END ITEM | | | ALC<br>1 | | ACCOUNT NO<br>5D7892 |
| QTY | SERIAL NUMBERS | | RECEIPT | | | TRANSFER | | | LOAN DATA | | ON HAND |
| | BEGIN | END | ACCOUNT | DATE | SERIAL NUMBER | ACCOUNT | DATE | SERIAL NUMBER | FROM | DURA TION | BALANCE |
| 1 | | 8125 | 5BE001 | 9244 | 00062 | | | | | | |
| 1 | | 9035 | 5BE001 | 9244 | 00062 | 241120 | 9305 | 00110 | NAVY | 120 DAYS | |
| 1 | | 10354 | 5BE001 | 9244 | 00062 | | | | | | |
| 1 | | 11345 | 5BE001 | 9244 | 00062 | | | | | | |
| 1 | | 66453 | 5BE001 | 9244 | 00062 | H/R<br>LT RJ<br>Lewis | 9260 | 5002 | | | |
| 1 | | 63234 | 5BE001 | 9244 | 00062 | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

DA FORM 2011-1-E
1 JUL 03

THIS FORM, TOGETHER WITH DA FORM 2011-E, 1 JUL 03
REPLACES DA FORM 2011-1, 1 NOV 77, WHICH IS OBSOLETE

(U) Hand receipt information will be recorded in pencil

**Figure 4-5. COMSEC Equipment Items Register.**
**Example for ALC 1 Equipment Accountable by Serial Number.**

| **COMSEC EQUIPMENT ITEMS REGISTER** (USING UNIT) | | | | | | | | | | | For use of this form, see TB 360-41; the proponent agency is AMC |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SHORT TITLE<br>E BDA | | | | NSN/MCN<br>59990124514 | | END ITEM<br>KG 30 101 | | | ALC<br>2 | | ACCOUNT NO<br>5DR 901 |
| Q T Y | SERIAL NUMBERS | | RECEIPT | | | TRANSFER | | | LOAN DATA | | ON HAND |
| | BEGIN | END | ACCOUNT | DATE | SERIAL NUMBER | ACCOUNT | DATE | SERIAL NUMBER | FROM | DURA TION | BALANCE |
| 3 | | | 5BE001 | 9172 | 00026 | | | | | | 3 |
| 1 | | | | | | (T)<br>5BE001 | 9181 | 0030 | | | 2 |
| 1 | | | 5BE001 | 9213 | 00035 | H/R<br>1LT Franks | 9214 | 5662 | | | 3 |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

DA FORM 2011-1-E
1 JUL 03

THIS FORM, TOGETHER WITH DA FORM 2011-E, 1 JUL 03
REPLACES DA FORM 2011-1, 1 NOV 77, WHICH IS OBSOLETE

*Hand receipt information will be recorded in pencil.

**Figure 4-6. COMSEC Equipment Items Register.**
**Example for ALC 2 Items Accountable by Quantity.**

## 4.8 CONTROL OF KEY TAPE SEGMENTS.

(U) The following guidelines are applicable to the control of key tape segments.

**4.8.1 (U) Digraph Code for COMSEC Key.** Completion of the COMSEC Material Disposition Record (DA Form 5941-E) is self-explanatory except for blocks 6, 7, 8 and 10. The information for these entries is contained in a two-letter code digraph to the left of the short title on the tape leader. The first letter explains the number of keys, the copies of the keys, and total number of segments. The second letter gives the cryptoperiod. An example would be: **GC**, (digraph: key information and cryptoperiod).

**a. (U)** If the first letter on the tape leader matches the one in the first column, the canister holds the number of keys, copies and total segments listed:

| | Copies Keys | Total of Keys | Seg. |
|---|---|---|---|
| A | 31 | 1 | 31 |
| B | 5 | 3 | 15 |
| C | 1 | 5 | 5 |
| D | 6 | 5 | 30 |
| E | 5 | 1 | 5 |
| F | 1 | 10 | 10 |
| G | 16 | 1 | 16 |
| H | 1 | 31 | 31 |
| I | 1 | 15 | 15 |
| J | 26 | 1 | 26 |
| L | 35 | 1 | 35 |
| M | 2 | 1 | 2 |
| N | Contact | CONAUTH | |
| O | 68 | 1 | 68 |
| Q | 34 | 1 | 34 |
| R | 4 | 10 | 40 |
| S | 75 | 1 | 75 |
| T | 12 | 1 | 12 |
| U | 65 | 1 | 65 |
| V | 62 | 1 | 62 |
| W | 1 | 65 | 65 |
| Z | 15 | 5 | 75 |

**b.** (U) The second letter of the two-letter code is the cryptoperiod. If the second letter matches the one in the first column, the cryptoperiod is as stated in the following:

**Cryptoperiod**

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

**4.8.2 (U) Local Accounting for COMSEC Key.**

**a. (U) Use of the COMSEC Material Disposition Record (DA Form 5941-E) for Local Accounting of Key Tape Segments.** DA Form 5941-E is a reproducible form in an easy-to-use format, which will be used to record the issue, use and destruction of key tape segments (a facsimile of this form is authorized). Use this disposition record as a management tool in the local accounting of key tape segments. A copy of the key disposition record will be retained upon destruction of key tape segments to identify those personnel actually performing destruction. Once the key tape segment disposition record has any information entered on it that reveals classified information (e.g., date exposed, date destroyed), it will be marked with the appropriate classification, not lower than CONFIDENTIAL, in letters larger than the largest letters printed on the form IAW AR 380-5. However, the disposition record will not be stamped as classified if the key tape is unclassified. The custodian will maintain the completed DA Form 5941-E (or facsimile thereof) on file until the SF 153, which lists its disposition, is destroyed.

**b. (U) Use of Key Tape Canisters and Segments.** The CONAUTH is responsible for determining the quantity of key tape canisters required and their distribution within the cryptonet (refer to AR 380-40 and Chapter 3 this TB). The following procedures apply to the use of key tape canisters:

(1) (U) Key tape canisters will be hand-receipted to the user as an unused, complete canister. In addition to the SF 153 hand receipt, a disposition record will also be provided to the user for recording the destruction of used key tape segments.

(a) (U) Single copies of key tape segments used for secure communications should be destroyed immediately after successful encryption of communications has been achieved. When this is not possible, the key segment must be destroyed not later than 12 hours after supersession.

(b) (U) Used key tape segments having multiple copies (i.e., 1/2, 1/3, etc., located at the lower right side of key tape canister) will be destroyed immediately after successful encryption of communications. The unexposed duplicated segment(s) will be maintained for use (backup in case of systems failure) within the cryptoperiod and destroyed no later than 12 hours after the supersession date. If due to system failures all duplicate copies are used and destroyed, the last copy may be retained until the end of the cryptoperiod.

(c) (U) Inter-theater COMSEC Package (ICP) will be handled IAW the ICP Manager Red Book.

(2) (U) The COMSEC Custodian, along with a properly cleared witness, may destroy un-issued segments as the segments are superseded or as entire editions. Key that is designed for off-the-air applications has no prescribed cryptoperiod and may be used until no longer serviceable.

(3) (U) It is not mandatory that a security container (i.e., vault/GSA Safe) be opened for the sole purpose of destroying individual key tape segments that are in protective packaging

(4) (U) The user, along with a cleared witness, will destroy key tape segments upon supersession and record the destruction on the DA Form 5941-E (a signature, initial, or printed name will be inserted in the “issued” block of the local destruction record). These entries are required each time a segment(s) is (are) pulled. For example, if the user is using a monthly canister but doesn’t bring up the net until day four, the first entry would reflect “1-4.” This practice could occur at any time during the month. See Figure 4-7 for a sample of a DA Form 5941-E. The use of diagonal lines or quotation marks is not authorized. Retain the DA Form 5941-E with the associated tape canister until all tape segments have been destroyed.

(5) (U) Disposition records and the empty key tape canister or key tape canister of unused segments will be returned to the COMSEC Custodian. The custodian will return the hand receipt (SF 153) to the user.

(6) (U) The COMSEC Custodian will retain the DA Form 5941-E, or other form of local destruction document, until the remaining segments in the key tape canister are destroyed in support of the Consolidated Destruction Report. The custodian will attach all local destruction documents directly to the Consolidated Destruction Report to ensure the records are not destroyed prematurely as well as for easy access for review by the custodian, an auditor, or an inspector. Should a custodian discover that a Local Destruction Report is not on file to support a Consolidated Destruction Report, it must be reported immediately as an incident IAW AR 380-40, paragraph 7-3a.

(7) (U) The user will immediately notify the CONAUTH (by secure means) and the COMSEC Custodian if a key tape canister or segment is lost, stolen, or in any way subjected to any type of COMSEC Incident.

(8) (U) Empty key tape canisters will be destroyed by the COMSEC Custodian whenever practical (the custodian may require the user destroy the empty canister based on geographical locations or high quantities). If there are any key tape production problems discovered with the canister, report the incident IAW Chapter 7.

**c. (U) Physically Accounting For Used Key Tape Segments.** Use the following two checks to account for used key tape segments. The first check is done at the operational area before each shift is relieved to ensure that all used key tape segments were placed in destruction channels (i.e., placed in a lock box or destroyed). The second check is made by the COMSEC Custodian to verify that disposition records reflect the correct material issued to the user as shown on the hand receipt.

(1) (U) *Operational Check.* Shift-to-shift accountability will be accomplished using the DA Form 2653-E (included in Appendix D) in conjunction with the key tape segment disposition record (see figures 4-9 and 4-10). Ensure segments are destroyed or physically sighted by verifying the next upcoming segment in the key canister window. All accounting for used key tape segments must take place before the responsible shift is relieved. If a key tape segment or canister is misplaced, it must be recovered before the personnel involved have left the area. In the event material cannot be located, notify the COMSEC Custodian immediately. If a security container has not been opened during a shift, the operational check is not required.

(2) (U) *Custodian Check.* The COMSEC Custodian is responsible for the key tape segment accounting procedures and the physical security of used key tape segments. If the COMSEC Custodian does not authorize users to perform destruction functions, then he/she must impose sufficient security checks of the material to ensure accurate accounting procedures are maintained. This should be clearly outlined in the hand-receipt holder briefings and local SOPs, when such SOPs are established.

**d. (U) Premature Exposure of Key Tape Segments.** The following procedures apply when key tape segments in a canister are prematurely exposed: (e.g., (a) User pulls segment one; however, by accident, does not realize that segment two was also pulled; (b) User pulls segment from the wrong canister).

(1) (U) The first person that becomes aware that a key tape segment has been prematurely exposed must initiate action to notify the CONAUTH IAW Chapter 7.

(2) (U) While awaiting disposition instructions, the exposed key tape segment must be secured against unauthorized access.

(3) (U) Key tape segments accidentally exposed, and having multiple copies, will be destroyed unless it is the last copy, which will be safeguarded and stored in accordance with its classification until used.

**4.8.3 (U) Authorized Exposure of Keying Material.** This subparagraph applies only to physical hard copy key.

**a. (U)** Units/elements deploying under real-world crisis/contingency scenarios may download the current edition plus the minimum amount of key material necessary for the immediate crisis/contingency: up to a maximum of 90 days of keying material may be downloaded into a DTD. Fill devices such as the KYK-13/KYX-15(A) will not be used for this purpose. Request for extension in excess of 90 days must be submitted through command channels to HQDA DCS, G-2 and subsequent approval by the NSA

**b. (U)** Units deploying in other than crisis/contingency situations should limit the number of segments loaded into the DTD to those required for the mission.

**c. (U)** The CONAUTH must authorize exposure of key for downloading into DTDs and notify the COMSEC Custodian, in writing, of the material to be downloaded.

**d. (U)** When duplicate key is on hand, the exposed (hard copy) key will be destroyed immediately after successful loading into the DTD. The DTD will have the CIK removed whenever the DTD is not in use.

**e. (U)** Immediately after loading the DTD, place the exposed segments, along with a copy of the approval from the CONAUTH, in an envelope. Seal the envelope. On the outside of

the envelope, annotate the contents and the classification of the contents, and then sign the envelope to reflect verification of the contents.

**f. (U)** When performing a daily shift inventory or an SAIR, it is not necessary to unseal the envelope for the purpose of physically inventorying the segments. However, during a CCIR or a CSLA Audit, the incoming COMSEC Custodian or auditor must physically view the segments. A new envelope must then be prepared as stated in the preceding paragraph.

**g. (U) The loading of key into a DTD to satisfy emergency mission requirements, as provided for in paragraph 4.8.3, is not considered premature exposure of key and is not a reportable COMSEC Incident**.

**COMSEC MATERIAL DISPOSITION RECORD**
For use of this form, see TB 380-41; the proponent agency is AMC.

| 1. SHORT TITLE | 2. REG/EDIT | 3. SEC CLASS | 4. SERIAL NUMBER | 5. EFFECTIVE DATE |
|---|---|---|---|---|
| USKAT 1234 | A | S | 4321 | 1JAN03 |

| 6. NR OF KEYS | 7. NR OF COPIES | 8. TOTAL NR OF SEGMENTS | 9. CONTROLLING AUTH | 10. CRYPTO PERIOD |
|---|---|---|---|---|
| 31 | 1 | 31 | CDR 15K BDE | MONTHLY |

| 11. SEGMENT/DAY | 12. ISSUED TO/DATE USED | 13. DESTROYED BY/DEST DATE | 14. WITNESSED BY/DATE |
|---|---|---|---|
| 1 | Dennis R. Hilliard 1 Jan 03 | Dennis R. Hilliard 2 Jan 03 | Teresa B. Moreno 2 Jan 03 |
| 2 | Dennis R. Hilliard 2 Jan 03 | Dennis R. Hilliard 3 Jan 03 | Teresa B. Moreno 3 Jan 03 |
| 3-5 | Dennis R. Hilliard 5 Jan 03 | Dennis R. Hilliard 5 Jan 03 | Teresa B. Moreno 5 Jan 03 |
| 6 | Dennis R. Hilliard 6 Jan 03 | Dennis R. Hilliard 7 Jan 03 | Teresa B. Moreno 7 Jan 03 |
| 7 | Dennis R. Hilliard 7 Jan 03 | Dennis R. Hilliard 8 Jan 03 | Teresa B. Moreno 8 Jan 03 |
| 8-31 | Dennis R. Hilliard 31 Jan 03 | Dennis R. Hilliard 1 Feb 03 | Teresa B. Moreno 1 Feb 03 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**DA FORM 5941-E, JUL 03**

See paragraph 4.8.2 for guidance regarding the classification marking of this form.

**Figure 4-7. COMSEC Material Disposition Record (DA Form 5941-E)**

# 4.9 PREPARATION OF COMSEC MATERIAL REPORT (SF 153).

**4.9.1 (U) General.**

**a. (U)** The COMSEC Custodians of Traditional COMSEC accounts will manually report COMSEC material transfers, inventories, conversions, special possessions and destructions using the COMSEC Material Report, SF 153. This form is for use in printed hard copy, automated reproduction, electronic transmission, or Automatic Data Processing (ADP) facsimile, provided all required data entries are included. It is used for all types of COMSEC accounting transactions including the hand receipt of material.

*LCMS WORKSTATION accounts will print a hard copy for **record** purposes.*

**b. (U)** SF 153s listing Positive Control Material (PCM) will be marked IAW the CJCSI 3260.01 publication.

**c. (U)** Reports will be signed in black or blue ink. Legible carbon-imprinted signatures on the SF 153 are acceptable. Multiple pages will be signed on the last page. <u>All other pages will be initialed or signed.</u>

**d. (U)** Individual(s) signing verifying deletions or corrections to an SF 153 will initial the report in black or blue ink.

**e. (U)** When a corrected voucher (SF 153) is submitted to the COR, it will be conspicuously annotated to reflect that it is a corrected copy, and it will be assigned the same Julian date and voucher number as the original voucher submitted to the COR.

**4.9.2 (U) SF 153 General Completion Instructions.**

**a. (U) Block 1.** Place an "X" in the appropriate sub-block for the type of report or action being completed: Transfer Report, Inventory Report, Destruction Report, Hand Receipt, or Other. The "OTHER" sub-block is used when preparing other manual reports such as a Special Possession Report, Conversion Report, Issue of ALC 4 material, etc. When the "OTHER" sub-block is used, indicate the type of report. When the "INVENTORY" sub-block is annotated, enter the type of inventory above the title line (see Table 4-7 and Figure 4-8).

**b. (U) Block 2. From.** Enter the complete official mailing address and the COMSEC account number under "ACCT NO."

**c. (U) Block 3. Date of Report.** Enter the calendar date the report is completed. The year, month, and day, as shown, will be used.

**d. (U) Block 4. Outgoing Number.** Enter the Julian date and voucher serial number (e.g., 9181-0003) for outgoing transactions.

**e. (U) Block 5. Date of Transaction.** Enter the calendar date on which the transaction occurred (used for hand receipt and Incoming).

**f. (U) Block 6. Incoming Number (optional).** Enter the Julian date and voucher serial number.

**g. (U) Block 7. To.** Enter the complete official mailing or physical address and the receiving COMSEC account under "ACCT NO," if applicable, as follows:

(1) (U) Transfer Report. Enter the physical address and the COMSEC account number of the gaining account.

(2) (U) For COMSEC accounting reports addressed to the COR, see Appendix F.

(3) (U) Hand Receipt (for Manual COMSEC Accounts only). Enter the name and official address of the individual receiving the COMSEC material. For TS material, only the name of the primary Hand Receipt Holder (block 15) is required.

**h. (U) Block 8.** For information only.

**i. (U) Block 9. Short Title/Designation Edition.** Enter short titles in alphanumerical sequence starting on line one. Omit the "TSEC" prefix/suffix. All entries will be single-spaced. The last line will be followed by the entry "NOTHING FOLLOWS" in upper case letters. In the following circumstances a mandatory statement will be entered below the "NOTHING FOLLOWS" entry:

(1) (U) COMSEC material is received without accompanying Transfer Report.

(2) (U) A sudden permanent departure or unauthorized absence of the COMSEC Custodian has occurred.

(3) (U) COMSEC equipment loaned to another service or agency. Indicate the expected loan duration (number of days) and purpose of loan.

(4) (U) Reporting a change or short title and/or serial number when COMSEC equipment has been converted after application of a Modification Work Order (MWO).

(5) (U) Reporting COMSEC material that was not previously accounted for by the COMSEC account.

(6) (U) Repayment or loan to another service or agency. Refer to original loan transaction to verify original equipment.

(7) (U) Permanent transfer of COMSEC material to a service or agency outside the Army. Include the following information:

(a) (U) Authority for transaction. Assets will not be transferred to a non-Army service or agency without written CSLA approval.

(b) (U) Indicate the transaction is a transfer loan or the repayment of a loan.

(c) (U) COMSEC shipment received incomplete.

(8) (U) A Consolidated Destruction Report requires a certification statement as found in paragraph 4.19.5b(1)(b).

(9) (U) Destruction of PCM requires a statement be inserted as shown in paragraph 4.19.5b(4).

**j. (U) Block 10. Quantity.** Enter quantity of each line entry.

**k. (U) Block 11. Accounting Numbers.** Enter serial numbers for ALC 1 material. When serial numbers for a line entry are in a series, the beginning number will be entered in the BEGINNING column and the last number will be entered in the ENDING column. When the serial numbers are not in series or the quantity is 1, enter the single serial number in the ENDING column (the CMCS can pick-up no more than an 11-digit serial numbers; therefore only the last 11 digits should be used).

**l. (U) Block 12. ALC**. Enter the ALC for each line entry.

**m. (U) Block 13. Remarks.** Make an entry when appropriate or when directed in specific report instructions.

**n. (U) Block 14. The Material Hereon has been.** Place an "X" in the Received, Inventoried, or Destroyed block.

**o. (U) Block 15. Signature of Authorized Recipient.** The COMSEC Custodian's hand-written signature and typed or stamped name, as shown on the CARP, is entered here. In the absence of the COMSEC Custodian, the alternate COMSEC Custodian will sign the transaction.

**p. (U) Block 16. Signature and Typed or Stamped Name.** The COMSEC witness will sign the SF 153. If the signature of a witness is required, check the WITNESS block.

**q. (U) Block 17.** Enter page numbers, classification of document, and if the SF 153 is reportable to the COR, Reports Control Symbol (RCS AMC-877).

# Table 4-7. COMSEC Material Report (SF 153)

## Additional Instructions

| TRANSACTION Block 1 | SITUATION | SPECIAL INSTRUCTIONS | BLOCK 15 | BLOCK 16 | BLOCK 17 |
|---|---|---|---|---|---|
| **Transfer** | COMSEC Material received without a Transfer Report. | After "Nothing Follows," indicate circumstances including package number, date of receipt, etc. Example: "Received via Defense Courier Service package TV604532, 30 May 99 from 208th Commo Sqdn Travis AFB, CA. Contacted shipper to obtain entries for blocks 3 and 4." | Signed by receiver of the shipment | | |
| **Transfer** | COMSEC material received from another service or agency. | | Signed by receiver of the shipment | | |
| **Inventory - Manual Change of Custodian** | Transfer of accountability from one COMSEC Custodian to another. | The outgoing number in Block 4 will use CUST as the document serial number. Example: 9234-CUST | Signed by incoming COMSEC Custodian | Signed by outgoing COMSEC Custodian | RCS AMC-877 |
| **Inventory - Special** | Unexplained absence of COMSEC Custodian | After "Nothing Follows," state the reason. Example: "Inventory submitted IAW TB 380-41 due to the sudden permanent departure of the former COMSEC Custodian." The outgoing number in Block 4 will use "CUST" as the document serial number. Example: 9234-CUST | Signed by COMSEC Custodian | Signed by authorized witness | RCS AMC-877 |
| **Inventory - Special** | Movement of COMSEC account. | After "Nothing Follows," state "Inventory submitted IAW TB 380-41 due to movement of the COMSEC Account." | Signed by COMSEC Custodian | Signed by authorized witness | RCS AMC-877 |
| **Inventory – Special Possession** | COMSEC Material found and not on the COMSEC Account records. | After "Nothing Follows," describe the circumstances. Example: MSG IAOPS-QP-OP, INSCOM 101400Z Apr 99, SUBJ: COMSEC Insecurity of Closed Case No 9-148KK, for loss of COMSEC material listed above has been recovered. MSG SELCL-KP-OR, CSLA 140928Z Apr 99, granted Relief from COMSEC Accountability to COMSEC Account 5DK894. This special report re-established COMSEC accountability. | Signed by COMSEC Custodian or Alternate | Signed by authorized witness | RCS AMC-877 |
| **Destruction** | Normal destruction of regular or irregular superseded key | | Signed by COMSEC Custodian or Alternate | Signed by authorized witness | RCS AMC-877 |



FOR OFFICIAL USE ONLY

| Table 4-7. COMSEC Material Report (SF 153) (Cont.) Additional Instructions | | | | | |
|---|---|---|---|---|---|
| **Destruction - Consolidated** | Hand Receipt Holder provides the COMSEC Custodian with destruction reports of an entire COMSEC item (e.g., edition) that has been destroyed and to show that the 2 people signing the report have personally destroyed all material | COMSEC Custodian consolidates the destruction reports received from the Hand Receipt Holder(s) into *one* destruction report. After "Nothing Follows," enter either the statement in paragraph 4.19.5b(1)b, or for a PCM destruction, the statement in paragraph 4.19.5b(4). | Signed by the COMSEC Custodian | | RCS AMC-877 |
| **Destruction – Consolidated Local Destruction** | Hand Receipt Holder reports the destruction of an entire COMSEC item (e.g., edition) has been destroyed and when the 2 people signing the report have personally destroyed all material | The outgoing number in Block 4 will use a local document number (5000 series). | Signed by the Hand Receipt Holder or authorized representative | | |
| **Hand Receipt** | Hand Receipt to an individual for normal key. | 1. Hand Receipts are not reportable to COR.<br>2. IR Cards will be annotated in pencil.<br>3. Two signatures required for TS and PCM material. 4. The outgoing number in Block 4 will use a local document number (5000 series). | Signed by Hand Receipt Holder | Signed by authorized witness if TS or PCM material involved. | |
| **Hand Receipt** | Hand Receipt for reproduced COMSEC Material | 1. Indicate days after the edition, ex: (Days 1-5). 2. Serial numbers will be the original serial number plus copy number (e.g., 100-1, 100-2). 3. The outgoing number in Block 4 will use a local document number (5000 series). | Signed by Hand Receipt Holder | | |
| **Other - Conversion Report** | Submitted to COR after a Change of Short Title or other authorized modification to COMSEC Material. | After "Nothing Follows," describe circumstances. Example: Conversion Report submitted after application of MWO 11-5810-280-35-3. | Signed by COMSEC Custodian | | RCS AMC-877 |
| **Other - Loan** | Temporary Loan to other service or agency. | After "Nothing Follows," provide:<br>1. Authority to Transfer: (Msg, Ltr, etc.).<br>2. Type of Loan: (e.g., Temporary).<br>3. Duration: (e.g., Not to exceed 120 days).<br>4. Ownership: (e.g., Army-owned Equipment).<br>5. Reason: (e.g., Loan is for test and equip will be returned to Army upon completion of test). | Signed by authorized loan recipient | | |

**COMSEC MATERIAL REPORT** (Classification) This form is FOR OFFICIAL USE ONLY unless otherwise stamped.

1. (X one)

☐ TRANSFER ☐ INVENTORY ☐ DESTRUCTION ☐ HAND RECEIPT ☐ OTHER (*Specify*)

2. ACCT. NO.

**FROM**

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

4. OUTGOING NUMBER

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

6. INCOMING NUMBER

7. ACCT. NO.

**TO**

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 / DESIGNATER - EDITION | | 10 QUANTITY | 11. ACCOUNTING NUMBERS BEGINNING | ENDING | 12. * ALC | 13. REMARKS |
|---|---|---|---|---|---|---|
| 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. | | | | | | |
| 32. | | | | | | |
| 33. | | | | | | |
| 34. | | | | | | |

For ease in processing/preparing SF 153 the following listing of Tables and Figures is provided for your information.

| | |
|---|---|
| Table 4-2 | Accounting Reports |
| Table 4-3 | Transfer/Receipt Reports |
| Table 4-4 | Destruction Reports |
| Table 4-5 | Inventory Report (Traditional Accounts) |
| Table 4-6 | Modification of Other Services Voucher Numbers |
| Table 4-7 | COMSEC Material Report (SF 153) |
| Figure 4-1/2 | COMSEC Material Voucher Control Registers |
| Figure 4-3/4 | COMSEC Aid Items Register |
| Figure 4-5/6 | COMSEC Equipment Items Register |

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 USA |

17. FOR DEPARTMENT OR AGENCY USE ONLY

RCS AMC-877 (as required) (classification) Page of Pages*

NSN 7540-00-935-5861
Previous editions are obsolete
ORIGINAL

This form is FOR OFFICIAL USE ONLY unless otherwise stamped.

153.130

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

**Figure 4-8. COMSEC Material Report (SF 153)**

# 4.10 TRANSFER OF COMSEC MATERIAL.

**4.10.1 (U) Transfer of COMSEC Material Between COMSEC Accounts.** Accountable COMSEC material will be transferred between COMSEC accounts by use of a Transfer Report (SF 153). COMSEC material will be listed exactly as it appears on the account records. Table 4-3 provides distribution information for copies of the Transfer Report. This **does not** pertain to CCI equipment.

**4.10.2 (U) Responsibilities.**

**a. (U)** The shipping COMSEC Custodian is responsible for:

(1) (U) Obtaining the official address of the receiving COMSEC account.

(2) (U) Forwarding to the COR copies of all accountable Transfer Reports.

(3) (U) Initiating a follow-up with the receiving account if the signed Transfer Report is not returned within the following time periods:

(a) (U) 30 days for CONUS shipment between COMSEC accounts.

(b) (U) 45 days for shipment between CONUS-to-overseas, overseas-to-CONUS, or theater-to-theater.

(c) (U) 60 days for shipment to National Guard accounts, Army Reserve, or other governmental agencies.

(4) (U) Each follow-up should be 15 days apart. If, on the third follow-up, receipt of the material shipped cannot be confirmed, notify the COR and request assistance to resolve the problem. If the problem cannot be resolved, the shipping COMSEC Custodian will submit a COMSEC Incident Report (refer to Chapter 7 of this TB).

**b. (U)** The receiving COMSEC Custodian is responsible for signing and mailing a signed Transfer Report to the shipping COMSEC Custodian within 2 working days after receipt of material.

# 4.11 LOCAL ACCOUNTING FOR COMSEC MATERIAL.

**4.11.1 (U) Responsibilities.**

**a. (U) Material Availability.** COMSEC Custodians are responsible for making COMSEC material readily available to qualified users. Material remaining under the COMSEC Custodian's control for use by other persons does not require a hand receipt or other issue/transfer action.

**b. (U) Positive Control Material (PCM).** Local accounting for PCM will be as directed by CJCSI 3260.01 Publication.

**4.11.2 (U) ALC 1 and 2 COMSEC Material.** Local accounting procedures will provide for the following:

**a. (U) Clearance/Need to Know.** Before issuing or hand-receipting material, the COMSEC Custodian will ensure that the recipient is properly cleared and has a need-to-know. Upon release of the material, responsibility for safeguarding the material is passed on to the individual who takes possession. However, the COMSEC Custodian is still accountable to the COR for centrally accountable material that is hand-receipted to users.

**b. (U) Release.** COMSEC Custodians will normally release material on hand receipt using an SF 153. A DA Form 2407 or DA Form 5504 (Maintenance Request) may be used as a hand receipt when COMSEC equipment is turned in to a maintenance facility for repair and return. If it is later determined that the equipment must be evacuated by the CLSF to another facility, the accountable custodian will prepare and submit a Transfer Report (SF 153). When hand receipting TOP SECRET material, two properly cleared individuals must sign for the material.

**c. (U) Disposition.** For ALC 1 and 2 materials, the user will return the material to the COMSEC Custodian for destruction or other disposition, unless directed by the COMSEC Custodian to destroy the material. In such instances, the user will provide the custodian with an SF 153 or DA Form 5941-E Destruction Report.

**4.11.3 (U) Hand Receipting COMSEC Material.**

**a. (U)** The issuance of COMSEC material to individuals on a valid hand receipt is a transfer and delegation of responsibility to those individuals for the material entrusted to them. Accountability for that material remains exclusively and singularly with the COMSEC Custodian. **Responsibility** is defined as the obligation of an individual to ensure the U.S. Government property (COMSEC material) entrusted to his or her possession or supervision is properly used by authorized individuals only, continuously protected and cared for, and that proper custody and safekeeping of the material on hand receipt is exercised at all times until it is returned to the custodian, or otherwise properly disposed of in accordance with this TB and reported as such to the custodian.

**b. (U)** Any individual authorized by the COMSEC Custodian, or the commander for whom the account is maintained, may be designated as a COMSEC material Hand Receipt Holder; provided the individual has a valid need for the material, and he/she is a U.S. citizen or a legal U.S. Resident Alien who possesses the necessary security clearance and the means (facilities) to properly secure and protect the material. That includes U.S. Government contractor personnel providing services to the U.S. military organizations both in CONUS and at overseas U.S. installations. In the absence of the COMSEC Custodian, Alternate Custodians will not hand receipt COMSEC material to individuals not previously authorized to be Hand Receipt Holders without prior approval from the commander.

**c. (U) Hand Receipt.** See Chapter 6 for additional procedures involving AKMS COMSEC Accounts.

(1) (U) When it is required to provide COMSEC material to an individual, the material will normally be hand-receipted using an SF 153. The material can be hand-receipted to the individual for a specific or indefinite period of time. The individual takes possession of the material and assumes responsibility for safeguarding it.

(a) (U) Under unusual conditions (e.g., conditions that may delay a tactical mission), hand receipt forms other than SF 153 are acceptable providing they contain the six basic information elements listed in paragraph 4.11.3.c(4)(b) on the item being hand-receipted.

(b) (U) A DA Form 3964 may be used to hand receipt COMSEC material to staff duty officers. Use the routing block to transfer accountability from one staff duty officer to another.

(2) (U) Accountable COMSEC material will not be hand-receipted between COMSEC accounts. COMSEC material may, however, be hand-receipted to individuals, including other COMSEC Custodians. This material will not be entered on the COMSEC account records of the Hand Receipt Holder.

(3) (U) The COMSEC Custodian will ensure all Hand Receipt Holders are properly briefed on the safeguarding, destruction, inventory and operating instructions for the material being provided. Hand Receipt Holders will sign a briefing statement prepared by the custodian attesting to the fact that he/she has been properly briefed. Hand Receipt Holders for TS material will have an appointed Alternate Hand Receipt Holder that is properly cleared for TS. This person must also sign the SF 153 hand receipt for all TS material issued by the custodian to maintain TPI controls.

(4) (U) Specific instructions for the preparation of hand receipts are as follows (see Figure 4-8 and Table 4-7):

(a) (U) Prepare only two copies of the hand receipt and assign a local voucher number.

(b) (U) Record the following information for material being hand-receipted:

- (U) Short title.
- (U) Edition.
- (U) Segments/Days (when authorized by the CONAUTH).
- (U) Serial numbers (beginning and ending).
- (U) Quantity.
- (U) ALC number.

(5) (U) Prior to taking possession of the material, the receiving individual will perform the following:

(a) (U) Inventory the material against what is listed on the hand receipt SF 153

(b) (U) Verify the presence of all pages of unsealed key material and publications. When large quantities of material are required to be inventoried or page-checked, the Hand Receipt Holder may cause the verification of the presence of all pages by having another properly briefed and cleared individual perform the page check and sign the Record of Page Checks page.

(c) (U) If required, the person signing in block 15 will make corrections to the SF 153 and initial all corrections.

(d) (U) Have the alternate Hand Receipt Holder (HRH) sign block 16 when TOP SECRET material is received from the custodian.

(6) (U) The issuing COMSEC Custodian will keep the original copy of the hand receipt.

(7) (U) The Hand Receipt Holder (the person signing the hand receipt) will keep the duplicate copy.

(8) (U) For reproduced material, prepare a hand receipt as indicated in Table 4-7.

(9) (U) A hand receipt file will be maintained by both the issuing COMSEC account and the receiving individual. These hand receipt files serve as the record of accountability and responsibility for all material issued on hand receipt. Upon return of the material, the original copy of the hand receipt will be removed from the file by the custodian and returned to the Hand Receipt Holder. A line will be drawn through the entry on the DA Form 4669-E, as shown in figure 4-2. Identification and disposition of hand receipt files will be IAW AR 380-40, Appendix C.

**d. (U) Posting to Items Register (IR) Cards.** When COMSEC material is hand-receipted to individuals, a pencil notation of the material hand-receipted will be made to the appropriate Items Register Card. Pencil notation permits erasing when the item is returned to the issuing account. If the hand receipt is of short duration (one to two days), recording of hand receipt information on IR Cards is waived. The combination of the hand receipt file and the IR Cards will provide the necessary material status information.

**e. (U) Hand Receipt Duration.** For accounting purposes, hand receipts will remain valid for as long as the holder has a need for the material, or as directed by the COMSEC Custodian. There is no requirement to renew or update valid hand receipts.

**f. (U) Hand Receipt Inventory.** All material on a hand receipt will be included in SAIRs and other inventories to the COR. The custodian will physically inventory accountable material held on hand receipt. When physical inventory is impractical, written verification from the Hand Receipt Holder is authorized. During tactical operations, field exercises, maneuvers, or adverse environmental conditions, hand receipts are accepted as proof of possession. When conditions permit, possession will be physically verified.

**g. (U) Sub-Hand Receipts**. When operational requirements so dictate, holders of material on hand receipt may (with written authorization from the COMSEC Custodian) sub-hand receipt the material to another individual. This authority will be recorded on the SF 153 hand receipt (see AR 380-40, paragraph 2-12.) KOV-14s may require the custodian to authorize sub-hand-receipting due to the large amount of cards anticipated in each COMSEC

account. If so, the custodian may use whatever documentation deemed necessary to retain accountability of material.

**h. (U) Reporting Destruction of Key Material.** When all key material issued to the Hand Receipt Holder has been destroyed, the signed copy of the destruction records for ALC 4 key will be retained in the Hand Receipt Holder's files. If the material is ALC 1 key, return the destruction certificate to the issuing COMSEC Custodian as proof of destruction. The COMSEC Custodian will retain (or modify) the hand receipt and retain the destruction record in the COMSEC account files. When local destruction records are not used, the Hand Receipt Holder will prepare a Destruction Report (two copies) using the SF 153. The signed original will be forwarded to the COMSEC Custodian and the remaining copy retained on file by the Hand Receipt Holder. DA Form 3964 (Classified Document Accountability Record) may be used to record and report destruction of key material per AR 380-5.

## 4.12 INVENTORY REQUIREMENTS FOR COMSEC MATERIAL.

### 4.12.1 (U) Inventory Requirements for COMSEC Accounts

**a. (U) Inventory at the COMSEC Account.** At the COMSEC account, a complete physical inventory will be performed as follows:

(1) (U) Centrally accountable COMSEC material (ALC 1, 2, and 6) will be inventoried at 6-month intervals using a Semiannual Inventory Report (SAIR). An Audit or a Change of COMSEC Custodian Inventory Report (CCIR) also serves as a semiannual inventory.

(2) (U) ALC 4 and 7 materials will be inventoried upon change of custodian or annually.

(3) (U) When CSLA personnel audit COMSEC accounts, all COMSEC material is subject to inventory.

(4) (U) At other times when a special inventory may be required.

**b. (U) Inventory of Physical Material.** Inventories must be complete and accurate. An accurate COMSEC material inventory provides supply accountability and aids in the physical security of the COMSEC material. The COMSEC Custodian's signature on a Transfer-In, Inventory, or Destruction Report is a binding certificate that each item listed is correct and has been accurately accounted for, as noted in the report. The following inventory procedures are required:

(1) (U) Upon receipt of material or upon opening packages or containers, carefully examine packages, containers, and sealed unit packages for tampering.

(2) (U) When inventorying classified spare parts, which are packed in sets, in bulk, or unit package, use "hands on" inventory methods. This inventory requires the visual verification of the presence of the package or container and that the parts listed, quantity, and identification are as specified.

**c. (U) Inventory Upon a CCIR or SAIR.** Upon a change of COMSEC Custodian or a semiannual inventory, all COMSEC equipment will be inventoried as follows:

(1) (U) When inventorying COMSEC equipment that is known to be operating properly, it may be assumed that the equipment contains all assemblies and parts.

(2) (U) When inventorying equipment stored in a security area to which only the COMSEC Custodian and the Alternate(s) COMSEC Custodian have access, the "sight" inventory method may be used.

(3) (U) When inventorying equipment held in storage, it is recommended that equipment be checked for completeness. A qualified COMSEC maintenance technician should assist in this inventory of components.

**d. (U) Inventory Upon Transfer or Prior to the Destruction of COMSEC Material:**

(1) (U) Inventory both classified and unclassified COMSEC equipment, subassemblies, and components for completeness.

(2) (U) Page-check unsealed key material and publications.

**4.12.2 (U) CLSF Inventory Procedures**

**a. (U) Inventory Responsibility.** The account COMSEC Custodian or Alternate COMSEC Custodian and a witness should perform CLSF Inventories. However, other qualified personnel under the supervision of the COMSEC Custodian may perform inventories of large accounts or at major distribution centers.

**b. (U) Receipt of Inventory**. The following procedures are required for all CMCS accountable COMSEC material received at a CLSF for further distribution:

(1) (U) Carefully examine packages and containers for signs of tampering. If the package or container is free of tampering, do not open. An inventory of unopened packages and containers will be done by verifying the short title/edition, quantity, and serial accounting/register number on the label.

(2) (U) Larger packages (e.g., bulk-packaged COMSEC key material) may be opened for distribution of its smaller unit-packed contents. If the larger package has been opened, inventory its contents (smaller unit-packed packages). Large packages opened for distribution to smaller units may be resealed and remarked with the new quantity. There is no need to open smaller packages for inventories unless they show signs of tampering or have been opened. If a smaller unit-packed package has been found to be tampered with or opened, verify that the contents are complete.

(3) (U) Do not open packaged spare components for inventory. However, if the package has been opened, all individual classified components will be inventoried.

**c. (U) Periodic Inventory Requirements.**

(1) (U) Inventory large sealed units, which may include one or more pallets of material as a "total" sealed unit. When inventorying large sealed units, check all seals for tampering.

(2) (U) Inventory material which is stored loose (e.g., ALC 1 and ALC 2 keying material). Do **not** check equipment and subassemblies for individual parts.

(3) (U) Upon Transfer of COMSEC Material, check both equipment and individual components for completeness before packing for shipment. If the equipment or components have not been opened since they were received, the CLSF is not required to open and check these items. If equipment has been used, ensure it is zeroized prior to packing.

**4.12.3 (U) Daily and Shift-to-Shift Inventory of Key Material.** All centrally accountable COMSEC key will be inventoried to ensure continued protection and control. The DA Form 2653-E or locally produced report (which contains all the elements of the DA Form 2653-E) will be used to record the inventories.

**a. (U) Daily Inventory**. A daily inventory will be conducted in all accounts holding centrally accountable key regardless of quantity held. When key is stored in a security container that has not been opened since the previous inventory, it is not necessary to open the container for the sole purpose of conducting the daily inventory. Page checks of keying material are not required for daily inventories.

**b. (U) Shift-to-Shift Inventory.** Operational areas will maintain a written record of shift change inventories of cryptomaterial using DA Form 2653-E to document the transfer and physical control from the outgoing shift to the incoming shift. Locked security containers

do not require being opened for inventory purposes as stated in the preceding paragraph. Instructions for completing the DA Form 2653-E follow (also see Figure 4-9).

(1) (U) *Short Title*. Enter the short title and edition number for each item being inventoried in alphanumerical sequence.

(2) (U) *Qty*. Enter the required inventory quantity.

(3) (U) *Reg. No*. Enter the keying material register number(s) or serial number(s).

(4) (U) *Shift*. Use appropriate shift row when recording inventory (Shift 1, Shift 2, or Shift 3). If the account does not have shift changes and the safe is opened infrequently, the custodian may adjust the shift row to reflect three consecutive months vice shifts.

(5) (U) *Day of the Month*. Use the correct day of the month column when recording the inventory.

(6) (U) *Inventory Record*. Select the box that intersects the shift and the day of the month. If the inventory count agrees with the required quantity, place a check mark (4) in the inventory record. Checks will be annotated in the appropriate block upon receipt (transfer-in), daily/shift inventory and final disposition (transfer out and/or destruction).

(7) (U) *Initials*. If the inventory of all listed key material items is correct, place your initials in the box. Use the box which corresponds to the correct shift (1, 2, or 3) and day of the month. For TPI material, two (2) sets of initials are required (see Figure 4-10).

(8) (U) *Month*. Enter the month for which the inventory is being performed.

(9) (U) *Page Number*. Number each sheet consecutively.

(10) (U) *Number of pages*. Enter the total number of pages included for the entire month. Deletions and additions will be noted as shown in Figures 4-9 and 4-10.

(Classify as required)

**COMSEC ACCOUNT DAILY SHIFT INVENTORY**

For use of this form, see TB 380-41; the proponent agency is INSCOM.

**WHEN FILLED IN, THIS FORM WILL BE CLASSIFIED IN ACCORDANCE WITH TB 380-41**

| SHORT TITLE | QTY | REG. NO | SHIFT | DAY OF THE MONTH 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| USKAK 4606 (Q) | 1 | 1 | 1 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | | | 2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | | | 3 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| USKAK 7242 (GG) | 1 | 103 | 1 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | TEST | | | | | | | | | | | | | | | |
| | | | 2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | | | | | | | | | | | |
| | | | 3 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | | | | | | | | | | | |
| USKAY 3172 (FD) | 2 | 3244 3245 | 1 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | | | 2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | | | 3 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| USKAY Reg. 3395 (4-6) | 1 | 37206 | 1 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | | | 2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | | | 3 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| USKAK 3842 (AB) | 1 | 22 | 1 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | TEST | | | | | | | | | | | | |
| | | | 2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | | | | | | | | |
| | | | 3 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | | | | | | | | |
| USKAK 4606 (R) | 1 | 1 | 1 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | | | 2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | | | 3 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| USKAK 3842 (AC) | 1 | 23 | 1 | RECEIVED | | | | | | | | | | | | | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | | | 2 | | | | | | | | | | | | | | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | | | 3 | | | | | | | | | | | | | | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | | | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SHORT TITLE | QTY | REG. NO | DAY | 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 |
| MONTH JUNE 1992 | | SHIFT 1 | INITIALS | DM | DM | DM | DM | DM | DM | DM | DM | DM | DM | DM | DM | DM | DM | DM | DM | DM | DM | DM | DM | DM | DM | HR | HR | HR | DM | DM | DM | DM | DM | DM |
| PAGE NUMBER 1 | | SHIFT 2 | | EB | EB | EB | EB | EB | EB | EB | EB | EB | EB | EB | EB | EB | EB | EB | EB | EB | EB | EB | EB | EB | EB | AH | AH | AH | EB | EB | EB | EB | EB | EB |
| NUMBER OF PAGES 1 | | SHIFT 3 | | KM | KM | KM | KM | KM | KM | KM | KM | KM | KM | KM | KM | KM | KM | KM | KM | KM | KM | KM | KM | DR | DR | DR | KM | KM | KM | KM | KM | KM | KM | KM |

**DA FORM 2653-E** JUL 03

REPLACES DA FORM 1 OCT 68, WHICH WILL BE USED

**Figure 4-9. COMSEC Account – Daily Shift Inventory**

(Classify as required)

**COMSEC ACCOUNT – DAILY SHIFT INVENTORY**

For use of this form, see TB 380-41; the proponent agency is AMC

**WHEN FILLED IN, THIS FORM WILL BE CLASSIFIED IN ACCORDANCE WITH TB 380-41**

| SHORT TITLE | QTY | REG. NO | SHIFT | DAY OF THE MONTH 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| USKAK 4606 (Q) | 1 | 1 | 1 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | | | 2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | | | 3 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| USKAK 7242 (GG) | 1 | 103 | 1 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | DEST | | | | | | | | | | | | | | | |
| | | | 2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | | | | | | | | | | | |
| | | | 3 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | | | | | | | | | | | |
| USKAY 3172 (FD) | 2 | 3244 3245 | 1 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | | | 2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | | | 3 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| USKAY Reg. 3395 (4-6) | 1 | 37206 | 1 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | | | 2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | | | 3 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| USKAK 3842 (AB) | 1 | 22 | 1 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | DEST | | | | | | | | | | | | |
| | | | 2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | | | | | | | | | |
| | | | 3 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | | | | | | | | | |
| USKAK 4606 (R) | 1 | 1 | 1 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | | | 2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | | | 3 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| USKAK 3842 (AC) | 1 | 23 | 1 | RECEIVED | | | | | | | | | | | | | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | | | 2 | | | | | | | | | | | | | | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | | | 3 | | | | | | | | | | | | | | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | | | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| FOR TWO PERSON INTEGRITY (TPI) ONLY | | | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| JUNE 1992 | | SHIFT1 | 1 | MH | MH | MH | MH | MH | MH | MH | MH | MH | MH | MH | MH | MH | MH | MH | MH | MH | MH | MH | MH | MH | MH | MH | MH | MH | MH | MH | MH | MH | MH | MH |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | SHIFT2 | 1 | OG | OG | OG | OG | OG | OG | OG | OG | OG | OG | OG | OG | OG | OG | OG | OG | OG | OG | OG | OG | OG | OG | OG | OG | OG | OG | OG | OG | OG | OG | OG |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | SHIFT3 | 1 | GP | GP | GP | GP | GP | GP | GP | GP | GP | GP | GP | GP | GP | GP | GP | GP | GP | GP | GP | GP | GP | GP | GP | GP | GP | GP | GP | GP | GP | GP | GP |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SHORT TITLE | QTY | REG. NO | DAY | 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 |
| MONTH JUNE 1992 | | SHIFT 1 | INITIALS | OM | DM | OM | DM | DM | DM | OM | DM | OM | DM | DM | DM | OM | DM | OM | DM | DM | DM | OM | DM | OM | DM | HR | HL | HR | OM | DM | OM | DM | DM | |
| PAGE NUMBER 1 | | SHIFT 2 | | EB | EB | EB | EB | EB | EB | EB | EB | EB | EB | EB | EB | EB | EB | EB | EB | EB | EB | EB | EB | EB | EB | AH | AH | AH | EB | EB | EB | EB | EB | |
| NUMBER OF PAGES 1 | | SHIFT 3 | | KM | KM | KM | KM | KM | KM | KM | KM | KM | KM | KM | KM | KM | KM | KM | KM | KM | KM | KM | KM | KM | DR | DR | KM | KM | KM | KM | KM | KM | KM | |

**DA** FORM 1 NOV 74 **2653-R** REPLACES DA FORM 2653,1 OCT 67, WHICH WILL BE USED.

**Figure 4-10. COMSEC Account – Daily Shift Inventory (TPI)**

# 4.13 REPORTING PROCEDURES FOR INVENTORIES.

### 4.13.1 (U) COMSEC Account Semiannual Inventory Report (SAIR) for Traditional (Manual) Accounts.

**a. (U)** Traditional COMSEC accounts reporting to COR will receive a preprinted SAIR. If an SAIR is not forwarded to the account 6 months from the date of the last inventory performed, notify COR and the SAIR will be provided. Having received the SAIR, a 100% physical inventory of the account's holdings must be performed as of the cutoff (**preprinted**) date of the report. The report will have a minimum of three pages.

(1) (U) The first page consists of the header, also known as the address page.

(2) (U) The account's inventory listing as recorded by the COR will begin on the second page. Use this section of the preprinted report to conduct your inventory.

(3) (U) The last page of the report is the Certification/Correction page, commonly referred to as the C&C page. When an adjustment is required, the custodian must record the ADDITIONS or DELETIONS on this page (see Figure 4-11) in alphanumerical sequence. Verify the account's IR Cards against the preprinted inventory and physical inventory.

(a) (U) ADDITIONS to the C&C page represent accountable (ALC 1 and ALC 2) COMSEC material received **on or before** the cut-off date of report, but were not listed on the SAIR by the COR.

(b) (U) DELETIONS to the C&C page represent accountable (ALC 1 and ALC 2) COMSEC material which are listed on the preprinted SAIR, but, as of the cut-off date of the report, are not accounted for due to destruction, transfer, or non-receipt of material in-transit to your account.

(4) (U) After completing the 100% physical inventory and comparing the results to the SAIR and IR Cards, record all inventory adjustments on the C&C page. Forward one copy of the completed, signed, and dated C&C page to the COR. Place the second completed copy of the C&C page with a copy of the preprinted report in the account file. The C&C page has two functions:

(a) (U) It is used to certify that a physical inventory was performed, and that the COMSEC Custodian has possession or control of all material listed on the SAIR.

(b) (U) The C&C page also provides the means of recording corrections to the preprinted inventory list and to certify the corrections represent the current inventory status of the account.

**b. (U)** All ADDITIONS and DELETIONS must be substantiated by SF 153 supporting documentation submitted with the C&C page to the COR. Also, make sure that all corrections to the C&C page are annotated **in ink** and initialed by both people signing the report.

**c. (U)** A completed, signed, and dated copy of the C&C page from the SAIR (with supporting documentation) will be mailed to the COR within 45 days of the cut-off date of the report. Reserve and National Guard accounts are allowed an additional 15 days to submit the C&C page. Delinquent reports are monitored and will be traced through command channels.

**d. (U)** The C&C page completion instructions are as follows (see Figure 4-11).

(1) (U) *Additions.* For material received on or before the preprinted cut-off date, enter the shipper's voucher number for all material received and attach a copy of the voucher to the C&C page. However, if only a portion of the material listed on the shipper's voucher has been received, enter the material received individually on the C&C page as follows: Type or Print the word "ADDITIONS."

Under ADDITIONS, enter the following information for each item:

(a) (U) SHORT TITLE.

(b) (U) EDITION (not required for equipment).

(c) (U) QUANTITY.

(d) (U) BEGINNING and ENDING serial numbers (must agree with quantity).

(e) (U) ALC assigned by the NSA.

(f) (U) REMARKS. Indicate the Shipper's Voucher Number, Special Possession, etc.

(2) (U) *Deletions.* For material deleted before the preprinted cut-off inventory date, enter the outgoing voucher numbers and attach a copy of the vouchers to the C&C page. If only a portion of the material listed on the outgoing vouchers has been deleted, enter the deleted material individually on the C&C page as follows: Type or Print the word "DELETIONS." Under DELETIONS enter the following information for each item:

(a) (U) SHORT TITLE.

(b) (U) EDITION (not required for equipment).

(c) (U) QUANTITY.

(d) (U) BEGINNING and ENDING serial numbers (must agree with quantity).

(e) (U) ALC assigned by the NSA.

(f) (U) REMARKS. (Indicate the Outgoing Voucher Number (destruction, transfer, etc).

(g) (U) IN-TRANSIT MATERIAL. Incoming material that has been shipped, but not received by the COMSEC account (referred to as Incoming In-transit Material) is indicated on the preprinted SAIR by the shipper's voucher number in the "REMARKS" column. Reserve and National Guard accounts are allowed an additional 15 days to submit the C&C page. If this material has not arrived by the cut-off date, enter the shipper's voucher number under "DELETIONS" on the C&C page, and state "not received" in the "REMARKS" column (see Figure 4-11).

(3) (U) *Summary.* Following the last "ADDITION" and/or "DELETION" entry, record the statement "NOTHING FOLLOWS." If there were no "ADDITIONS" or "DELETIONS," record "NOTHING FOLLOWS" immediately under the "Voucher Number or Short Title" line at the top of the page.

**(U) Each line above the "NOTHING FOLLOWS" on a C&C page must be single-spaced.**

(4) (U) *Review of the CARP*. As a final step in the SAIR administrative process, the COMSEC Custodian will verify the current status of the account's CARP (see paragraph 2-5). If there are no changes, the custodian will prepare a short statement to that effect on the C&C Page just below the "NOTHING FOLLOWS" entry (e.g., "I have reviewed the CARP for COMSEC Account 5AXXXX dated [date of last submission] and certify that all data is current."). However, if the CARP requires updating, it must be revised immediately and a copy provided to the COR with the completed inventory (see Figure 4-11).

(5) (U) *Certification Signatures*. Once the C&C page has been completed, the COMSEC Custodian and a witness will sign and date both copies of the C&C page. In the event the COMSEC Custodian is not available (absent due to emergency, etc.), the C&C page will be signed and dated by the Alternate COMSEC Custodian and a properly cleared witness. Upon return of the COMSEC Custodian, the filed SAIR and C&C page will be reviewed for correctness. Following the review, the COMSEC Custodian will sign and date the file copy.

(6) (U) *Certification of Verification for Traditional accounts.* After processing the SAIR C&C page, and providing no discrepancies exist, the COR will issue a Certification of Verification.

UNCLASSIFIED

*Manager: 5*

CERTIFICATION/CORRECTION PAGE Account: 5D1234 RCS-AMC-877

SEMI ANNUAL INVENTORY REPORT

| Voucher Number or Short Title | Edition | Quantity | Beg Nr | End Nr | ALC | Remarks |
|---|---|---|---|---|---|---|
| ADDITIONS | | | | | | |
| USKAT 23 | A | 1 | 24 | 24 | 1 | |
| 616600-9021-8802 | | | | | | |
| DELETIONS | | | | | | |
| AKAT 54 | C | 2 | 37 | 38 | 1 | |

NOTHING FOLLOWS

"I have reviewed the CARP for COMSEC Account 5D1234 Dated (date of last submission) and certify that all data is current."

OR PROVIDE A CARP STATEMENT:

"A revised CARP for COMSEC Account 5D1234 is hereby provided to the COR IAW TB 380-41.

I HAVE INVENTORIED AND ASSUME ACCOUNTABILITY FOR THE MATERIAL LISTED ON THIS REPORT, AS SUPPLEMENTED ABOVE.

(COMSEC CUSTODIAN SIGNATURE) (DATE)
Pete Michaud
5 May 2003

(TYPED NAME AND GRADE)
Pete Michaud,
CW5

I HAVE WITNESSED THE INVENTORY OF THE MATERIAL LISTED ON THIS REPORT, AS SUPPLEMENTED ABOVE.

(WITNESS SIGNATURE) (DATE)
Larry Bryson
5 May 2003

(TYPED NAME AND GRADE)
Larry Bryson,
CW3

REPORT 5D1234-0059-KPD DATE OF REPORT 05/05/03 PAGE 3 OF 3 PAGES

UNCLASSIFIED

(U) Each line above the NOTHING FOLLOWS on a C&C page must be single-spaced.

**Figure 4-11. Preprinted Semiannual Inventory Report (SAIR) C&C Page**

**4.13.2 (U) COMSEC Account Semiannual Inventory Report (SAIR) for AKMS Accounts.** See Chapter 6 of this TB for instructions.

**4.13.3 (U) COMSEC Account Change of Custodian Inventory Report (CCIR) for Traditional Accounts.**

**a. (U)** It is the responsibility of the commander to select and appoint a new COMSEC Custodian (see paragraph 2.7.1.b for rank/grade restrictions) not later than 60 days prior to the departure of an incumbent custodian. A CARP with original signature must be provided to the COR. Alternate custodians may be changed whenever necessary and only an updated CARP is required.

**b. (U)** The outgoing COMSEC Custodian will request a printed Change of COMSEC Custodian Inventory Report (CCIR) by telephone, mail or e-mail from the COR (see Appendix F for POCs).

**c. (U)** Complete inventory reports of COMSEC account holdings are available by electronic means from the COR within one working day of the request. If the CCIR is requested to be transmitted electrically, a manually prepared C&C page must be prepared by the custodian and forwarded to the COR. Electronic requests will be sent to the COR that has been designated to support the account (Fort Huachuca, AZ, or Lackland Air Force Base, TX). See Appendix F for a listing of COMSEC POCs.

**d. (U)** In extreme circumstances, such as the death or immediate permanent departure of the COMSEC Custodian, an SF 153 may be submitted by the account as a manual CCIR. The SF 153 may also be used as a CCIR: if an account does not hold centrally accountable (ALC 1 or 2) material.

(1) (U) When the SF 153 is used as a CCIR, in block 1 of the form, mark "other" and fill-in "CCIR." In block 4, enter the Julian date the CCIR was completed and “CUST.” In block 9, enter one of the following statements, as applicable.

(a) (U) "This is an Emergency CCIR due to (the new custodian must complete this statement explaining the circumstances which justify the SF 153 CCIR submission to the COR).”

(b) (U) “This account holds no accountable ALC 1 or ALC 2 material.”

(2) (U) The Incoming COMSEC Custodian will sign the SF 153 in block 15, and the outgoing COMSEC Custodian will sign in block 16. In emergency situations when the outgoing custodian is not available to conduct a joint inventory with the new custodian, the commander will appoint a responsible, disinterested individual to assist the incoming custodian in conducting the inventory. That person will sign block 16 certifying as to the accuracy of the inventory being reported to the COR. A CARP must be forwarded with the manual CCIR.

**e. (U)** Both the outgoing and incoming COMSEC Custodians will conduct a physical inventory of all ALC 1, 2 and 4 material. All accounts will report ALC 1 and 2 material to the COR. A record of ALC 4 material will be maintained locally. Inventoried ALC 1 and 2 materials will be verified against the preprinted inventory report received from the COR. Changes will be reported on the C&C page.

**f. (U)** The C&C page will be completed in the same manner as the traditional SAIR C&C page, paragraph 4.13.1. However, the inventory will be worked to the date of signature.

**g. (U)** For a CCIR to be valid, the associated C&C page must be returned to the COR within 45 days from the date of the report (60 days for Reserves and National Guard). If it is not received within 45 days (or 60 days, as applicable), the COR will void the report. Upon verification/ reconciliation of the C&C page to the inventory report (providing no discrepancies exist), the COR will forward a Clearance of Former COMSEC Custodian memorandum or message to the COMSEC account.

**h. (U)** The new custodian will not sign for any COMSEC material received by the account prior to his/her official appointment date, as specified in the new CARP. After the appointment date and signature of the CCIR C&C page, the new custodian assumes full responsibility for all material, the facility, and the account records, in their existing condition.

**i. (U)** The former custodian will **NOT** leave the organization until a Clearance of Former COMSEC Custodian memorandum has been received from the COR.

**j. (U)** If the commander allows the COMSEC Custodian to depart the unit prior to clearance from COR, the commander assumes personal responsibility for the COMSEC account and any accounting irregularities that may exist.

**k. (U)** A CCIR also serves as a SAIR. The next SAIR will be scheduled six months from the CCIR signature date.

**4.13.4 (U) COMSEC Account Change of Custodian Inventory Report (CCIR) for AKMS Accounts.** See Chapter 6 this of TB for instructions.

**4.13.5 (U) Inventory of ALC 4 COMSEC Material.**

**a. (U)** All ALC 4 material will be locally inventoried annually and upon change of COMSEC Custodians (see Figures 4-12 and 4-13).

**b. (U)** The inventory date of ALC 4 material will be recorded by manual accounts on the IR Card. Instead of posting the inventory to the IR Card, an SF 153 may be used. The SF 153, if used, must be retained on file locally IAW AR 380-40, Appendix C. The signatures of the COMSEC Custodian and a witness are required on the SF 153 or IR Card, whichever is used, for the inventory of ALC 4 COMSEC material.

| COMSEC AIDS ITEMS REGISTER *(USING Unit)* | | | | | | | | For use of this form, see TB 380-41; the proponent agency is AMC | | |
|---|---|---|---|---|---|---|---|---|---|---|
| SHORT TITLE | | | | NSN/MCN | | LOCATION | | ALC | ACCOUNT NO | |
| KAM 220 | | | | 58 | | | | 4 | 5DR901 | |
| EDIT/REG | SERIAL NUMBERS | | RECEIPT | | DISPOSITION | | DEST/ISSUE DATE | DESTRUCTION CERTIFICATION | | |
| | BEGIN | END | FROM | DATE / SERIAL | TO | DATE / SERIAL | | 1. CUSTODIAN | 2. WITNESS | |
| A | 2458 | 2460 | 5BE001 | 9165 / 0025 | | | | 1 / 2 | | |
| | | 2459 | | | (T) 5BE001 | 9182 / 5030 | | 3 / 3 | | |
| CCIR 9287 | Gloria Henderson INCOMING CUSTODIAN | | | | Annette Geller OUT-GOING CUSTODIAN | | | 4 | | |
| | | | | | | | | 2 | | |

**Figure 4-12. Sample Completed CCIR COMSEC Aids Items Register (ALC 4) (DA Form 2011-E)**

| COMSEC AIDS ITEMS REGISTER *(USING Unit)* | | | | | | | | For use of this form, see TB 360-41; the proponent agency is AMC | | |
|---|---|---|---|---|---|---|---|---|---|---|
| SHORT TITLE SAM 67 | | | | NSN/MCN 581000U301094 | | LOCATION 8 | | | ALC 4 | ACCOUNT NO 5DR901 |
| EDIT/REG | SERIAL NUMBERS | | RECEIPT | | DISPOSITION | | DEST/ISSUE DATE | DESTRUCTION CERTIFICATION | | |
| | BEGIN | END | FROM | DATE SERIAL | TO | DATE SERIAL | | 1. CUSTODIAN | 2. WITNESS | |
| A | 109 | 110 | 5BE001 | 9338 0710 | | | | 1 2 | | |
| | Gloria Henderson | | | | Annette Geller | | | 3. 4. | | |
| | GLORIA HENDERSON COMSEC CUSTODIAN | | | | ANNETTE GELLER WITNESS | | | 5. 6. | | |
| | ANNUAL INVENTORY | | | | | | | 7. 8. | | |

**Figure 4-13. Sample of COMSEC Aids Item Register**
**ALC 4 Local Annual Inventory (DA Form 2011-E)**

**4.13.6 (U) Procedures to Change Alternate Custodians.** When there is a change of alternate custodians, a physical inventory of COMSEC material is not required. A new Alternate COMSEC Custodian may be appointed at any time. A modification to the CARP must be submitted to the COR. *A NEW DCS FORM 10 (SIGNATURE CARD) MUST ALSO BE SUBMITTED TO DCS.*

**4.13.7 (U) Special Inventory Report.**

**a. (U)** A manual or electronically prepared Special Inventory Report (SF 153) will be used to report the physical inventory of accountable COMSEC material charged to a COMSEC account under circumstances other than a routine change of custodian or SAIR (See to Figure 4-8, Table 4-7). These circumstances are as follows:

(1) (U) An unexplained temporary absence or permanent unauthorized absence of a COMSEC Custodian (see paragraph 4.13.3d).

(2) (U) Physical relocation/deployment of a Traditional COMSEC account within CONUS to an overseas command, from one overseas command to another overseas command, or moved from an overseas command to CONUS. (A special inventory will be conducted both prior to the move and again upon arrival at the destination). For AKMS accounts, see Chapter 6.

(3) (U) Unauthorized forced entry/access to a COMSEC Facility resulting in the loss, theft, damage, or destruction of COMSEC material.

**b. (U)** These inventory reports will be signed by the COMSEC Custodian or alternate COMSEC Custodian and a witness. The reason for the Special Inventory Report will also be annotated on the SF 153.

## 4.14 CONVERSION AND SPECIAL POSSESSION REPORTS.

**4.14.1 (U) Conversion Report.**

**a. (U)** An SF 153 Conversion Report is used to report a change in short title or serial number when COMSEC material or equipment components are converted from one configuration to another (see Figure 4-8, Table 4-7).

**b. (U)** Whenever a change in short title occurs on accountable COMSEC material, equipment or components, report the material changed to the COR. This change can result from:

(1) (U) Application of a modification work order (MWO) which affects the short title.

(2) (U) Converting end items to their components or components to an end item.

(3) (U) Direction from the COR.

**c. (U)** The SF 153 Conversion Report should include the ALC 4 components of the equipment when converting an end item to components or the components to an end item.

**d. (U)** The voucher number of the Conversion Report will be posted to reflect the disposition on the IR Cards for those items being deleted, and receipt for those items being added.

**4.14.2 (U) Special Possession Report.**

**a. (U)** An SF 153 Special Possession Report will be submitted to the COR when it is determined that centrally accountable COMSEC material on hand in the account has not been reported to the COR (see Figure 4-8, Table 4-7). In addition, Special Possession Reports will be required to document the following:

(1) (U) COMSEC material is discovered or found which is NOT listed in local COMSEC accounting records or COR records.

(2) (U) COMSEC material is "recovered" which was previously reported as lost, stolen or otherwise dropped from local COMSEC accounting records.

(3) (U) The assigned ALC for a COMSEC item is changed from locally accountable to centrally accountable, or from quantity accountable to serial number accountable.

**b. (U)** The COMSEC Custodian or alternate COMSEC Custodian and a witness will sign Special Possession reports. The reason for the Special Possession report will also be annotated on the SF 153.

## 4.15 ACCOUNTING FOR AND ENTERING AMENDMENTS TO COMSEC PUBLICATIONS.

(U) A listing of all COMSEC publications is contained in DA Pam 25-35. This pamphlet is available through STARPUBS. Post all amendments sequentially

**4.15.1 (U) Interim Amendments.** Post interim amendments received via message, memorandum or e-mail to the basic publication and record the entry on the Record of Amendments page sequentially. Copies of messages and memorandum amendments will be retained on file with the basic publication.

**4.15.2 (U) Reproductions of Interim Amendments.** CLSFs are authorized to reproduce classified and unclassified interim amendments for further distribution. Interim amendments will not be assigned an ALC. The transmission and receipt of these amendments will not be reported through the CMCS.

**4.15.3 (U) Official Amendments.**

**a. (U) General.**

(1) (U) Officially published amendments will be accounted for by the assigned ALC and recorded on individual IR Cards. These IR Cards are separate from the basic publications' IR Cards.

(2) (U) When a published amendment is received out of sequence, notify the office of issue. Only after receipt of the missing amendments will the remaining amendments be posted in chronological sequence based on the date of publication.

(3) (U) When an amendment is posted to a publication, the amendment is no longer a separate item; it becomes part of the basic publication.

(4) (U) For ALC 1 amendments, the COMSEC Custodian will prepare a Destruction Report. It is not necessary to list individual pages of residue (refer to Figure 4-8, Table 4-7).

(5) (U) For ALC 4 amendments, a Local Destruction Report must be prepared for the residue. This report will provide a complete audit trail for the ALC 4 material. Enter the destruction certificate on the IR Card for the amendment.

(6) (U) A record of page checks is required for accountable COMSEC publications. The cover of a basic publication will never be destroyed unless the amendment specifically directs such disposal.

**b. (U) Posting Amendments.**

(1) (U) Amendments must be posted within two working days after receiving the amendment. CLSFs are exempt from posting publications held in mission stock. In all other accounts, the COMSEC Custodian will personally post the amendment or supervise its posting.

(2) (U) Prior to posting, read the instructions contained in the memorandum of distribution for detailed instructions.

(3) (U) If pages are removed from the publication, recheck the removed pages prior to destruction against the list of superseded pages in the instructions. This is to prevent destruction of effective pages.

(4) (U) Record appropriate notations on the Record of Amendments page in accountable COMSEC publications. Memorandum and message amendments will be identified as depicted in this example: MEMO AMD#1 14 Jan 99, MSG AMD #2 141711Z Jun 99.

(5) (U) After inserting amendments, perform a page check of the total basic publication. BEFORE DESTROYING removed pages or any publication material, check all residue to make sure they agree with the list of pages authorized for destruction as listed in the instructions.

(6) (U) Record the page check(s) on the "Record of Page Checks," which is usually the first page of the document.

(7) (U) When preparing an SF 153 for posting to the IR Card (amendments require their own separate IR Card), be sure to report the destruction of the amendment, not the basic document.

**c. (U) Handling Residue (Superseded or Deleted Pages).** To prevent loss, place all residues, which are being held pending destruction, in a sealed envelope. Mark the envelope with the short title, serial number, and classification of the amendment. See paragraph 4.19 for mandatory destruction time frames.

## 4.16 ACCOUNTING FOR ALC 4 MATERIAL.

(U) ALC 4 material is not centrally accountable within the CMCS and, therefore, not reportable to the COR. Within the Army, ALC 4 material will remain under the CMCS control locally by COMSEC Custodians. COMSEC Custodian responsibilities include:

- (U) Inventory of ALC 4 material received, post receipt transactions to accounting records and maintain records of receipt.
- (U) Issue ALC 4 material to authorized users.
- (U) Record ALC 4 material issued by quantity on appropriate accounting record. Maintain records of distribution and destruction. This action constitutes final disposition of the material within the CMCS. The custodian is no longer responsible for the material in any manner.

**a. (U) COMSEC Publications.** Cryptographic Operational General Publications, maintenance and instruction documents, (KAGs, KAOs and KAMs) will be distributed, accounted for, and destroyed using the following procedures:

(1) (U) *Account Transactions.* An SF 153 will be used for accounting transactions between COMSEC accounts. All transfers of ALC 4 material will use local voucher numbers (5000-9999).

(2) (U) *Hand Receipts.* The COMSEC Custodian will hand receipt material using an SF 153 or other approved forms as listed in this TB. Material will either be returned to the COMSEC Custodian for destruction or other disposition, or at the custodian's direction, destroyed by the user. The user will record destruction on a Local Destruction Report (SF 153 or DA Form 5941-E) and provide a copy to the custodian.

(3) (U) *Sub-Hand Receipts.* When operational requirements so dictate, the COMSEC Custodian may authorize a Hand Receipt Holder to sub-hand receipt the material to another individual.

(4) (U) *Local Physical Inventory.* The COMSEC Custodian will conduct a local physical inventory annually and upon change of custodians.

(5) (U) *Destruction of Classified Material.* A properly cleared individual and witness will destroy classified material.

(6) (U) *Records of Transactions.* Records of transactions (to include transfers, inventories, and destruction) will be maintained locally and disposed of as directed by AR 380-40, Appendix C. These reports will not be submitted to the COR.

**b. (U) All Other COMSEC Material Designated ALC 4.** This category includes:

(1) (U) Modification work order (MWO) kits.

(2) (U) Certain training and exercise key.

(3) (U) Signal Operating Instructions (SOI), although not COMSEC material, fall in this category. After initial receipt of SOIs from the NSA or a CLSF, the COMSEC Custodian will prepare an IR Card to control the material until it is issued. Issue of SOI by the COMSEC Custodian constitutes the final action required within the CMCS (refer to AR 105-64 for further information). After issue, the SOI is handled and controlled as directed in AR 380-5.

**c. (U) User Control and Security.** Users will be instructed to handle and control ALC 4 material in a manner consistent with other national security information of the same classification. This control will include access control, shipment, storage, accounting, destruction, and incident or compromise reporting as directed by AR 380-5.

**d. (U) MWO Kits Accounting.** If any MWO kits are being held by accounts pending issue, these items will be recorded on IR Cards. This category of ALC 4 material does not have to be inventoried after it is installed.

**e. (U) TYAD and TCMO COMSEC Custodians.** COMSEC Custodians at TYAD and the TCMO are not required to obtain signed copies of Transfer Reports for outgoing shipments of ALC 4 COMSEC material. This exception does not apply to incoming shipments. ALC 4 material will be deleted from the records of these accounts after it has been prepared for shipment and made available for transportation.

## 4.17 REPRODUCTION OF COMSEC MATERIAL.

(U) The authority for local reproduction of COMSEC material is contained in AR 380-40. Reproduction of COMSEC material will normally be limited to key and publications in the form of extracts. Reproduction of complete documents will be limited to that necessary for cryptonet expansion. Written authority will be obtained from the CONAUTH prior to the reproduction.

(U) The reproduction of extracts is NOT reportable to the COR, but is locally accountable until destroyed. Transfer or issue of reproduced material will be accomplished using an SF 153. The following guidelines are provided to assist custodians in establishing local procedures for accountability of reproduced COMSEC material.

**4.17.1 (U) Accountable Publications.**

**a. (U)** Classify extracts per instructions or classification marking shown in the source publication. If the publication is not "portion" classified as required by AR 380-5, contact the proponent for the classification of the extract.

**b. (U)** Mark the extract with the exact words "Extract of____" (e.g., Extract of KA0 178A SN 155) and add a copy number to each reproduced extract, such as -01, -02, -03. Account for each extract by recording on a separate IR Card as shown in Figure 4-14. The IR Card will be maintained in the active file through final disposition of all reproduced copies.

**4.17.2 (U) Destruction of Reproducible Extracts.** Reproduced extracts must be destroyed no later than the date of supersession of the original document or deletion of the material from which the reproduction was made. Destruction can also be accomplished at any time prior to the supersession/deletion date when the reproduced extract is no longer needed.

**4.17.3 (U) Publications Prohibiting Reproduction.** When a publication prohibits its reproduction entirely, or in the form of extracts, only major training centers at which COMSEC courses of instruction are presented may reproduce extracts for restricted use as training aids.

**COMSEC AIDS ITEMS REGISTER** ***(USING Unit)***

For use of this form, see TB 360-41; the proponent agency is AMC

| SHORT TITLE | NSN/MCN | LOCATION | ALC | ACCOUNT NO |
|---|---|---|---|---|
| Reproduction of KAM 188 | | SAFE B3 | 1 | 5DE232 |

| EDIT/REG | SERIAL NUMBERS | | RECEIPT | | DISPOSITION | | DEST/ISSUE DATE | DESTRUCTION CERTIFICATION |
|---|---|---|---|---|---|---|---|---|
| | BEGIN | END | FROM | DATE SERIAL | TO | DATE SERIAL | | 1. CUSTODIAN 2. WITNESS |
| A | Pages 11-17 | 155-01 | Repro | 9193 | SFC M. Besmer | 5193 | | 1 |
| | | | | | | 5009 | | 2 |
| | Pages 11-17 | 155-02 | Repro | 9193 | (T) 5BR102 | 9196 | | 3. |
| | | | | | | 5011 | | 4. |
| | | | | | | | | 5. |
| | | | | | | | | 6. |
| | | | | | | | | 7. |
| | | | | | | | | 8. |

(U) All hand receipt information is entered in pencil.

**Figure 4-14. Local Accounting of Reproduced COMSEC Accountable Publication (DA Form 2011-E)**

## 4.18 MODIFICATION AND FABRICATION OF COMSEC MATERIAL.

**a. (U) Modification of COMSEC Material.** COMSEC equipment will not be altered in any way except on approval of HQDA and the National Security Agency (NSA). Requests to alter equipment will be sent to CSLA for processing and subsequent authorization. Requests will include:

(1) (U) Identification and serial numbers of the equipment affected.

(2) (U) Description of installation and usage.

(3) (U) Detailed justification explaining why modification is required.

**b. (U)** For authorized modifications to equipment refer to TB 750-38(C).

**c. (U) Fabrication of COMSEC Material.** The fabrication of COMSEC material, including unclassified CCI equipment, from components obtained through normal supply channels or any other source is prohibited.

**d. (U) Controlled Cryptographic Item (CCI).** For additional information on the control of CCI, refer to DA Pamphlet 25-380-2.

**e. (U) Adhesive Labels on COMSEC Equipment.** With NSA approval as to their location, adhesive labels may be affixed to COMSEC equipment for identification or other purposes.

## 4.19 DESTRUCTION OF COMSEC MATERIAL.

(U) This paragraph provides guidance and detailed procedures for the destruction of all CMCS-accountable COMSEC material, except electronic key, and other non-physical COMSEC material (see Chapter 6). Additional **Emergency Destruction Procedures** are in Chapter 5.

**a. (U)** Effective 1 January 2003, previously approved old-specification crosscut shredders (waste particle size 1/2" x 1/32") were no longer authorized for destroying ANY type of COMSEC material. The only shredder now authorized for destroying PAPER-BASED COMSEC materials is an approved crosscut shredder that meets the NEW standards and specifications established by the Committee for National Security Systems (CNSS) No. 16, as described in the NSA Evaluated Products List (EPL 02-01).

**b. (U)** The remaining methods for the destruction of paper-based COMSEC material defined below in paragraph 4.19.4 (i.e., burning, pulverizing and pulping, disintegrators, approved wet-pulping devices) are still considered as approved methods for the terminal destruction of paper-based COMSEC material.

***(U)*** *A short-term transition period has been established for the use of the old specification shredders until the new standard shredder can be purchased (see paragraph 4.19.4 c [1].)*

**(U) CAUTION: THE USE OF A SHREDDER AS A DESTRUCTION METHOD DOES NOT APPLY TO KEY TAPES. ALL KEY TAPES ARE CONSIDERED AS PLASTIC (MYLAR). FINAL DESTRUCTION OF KEY TAPES IS NOT, AND WILL NOT, BE AUTHORIZED EVEN IN THE NEW-SPECIFICATION CROSSCUT SHREDDERS. Key material with a short title beginning with USKAT (T=Tape) will only be authorized for destruction in approved disintegrators, by burning, or in NSA-approved Key Tape-specific Destruction Devices (KTDD). If a COMSEC account holds key tapes and burning is not possible, they MUST acquire an approved disintegrator or an approved KTDD to destroy these key tapes. See paragraph 4.19.4 below for key tape destruction.**

**4.19.1 (U) Routine Destruction Procedures.** All COMSEC Custodians are required to establish routine destruction procedures for the COMSEC products they manage. Destruction procedures must ensure complete destruction of material and an accurate system of accounting for destroyed material. Size and location of the COMSEC Facility, amount of material, personnel resources, and available destruction facilities will determine local destruction procedures.

**4.19.2 (U) Scheduled Destruction.**

**a. (U) Keying Material.** Destroy all superseded keying material, including key tapes, Modern electronic SDNS/FIREFLY Key such as TACLANE/ FASTLANE, one-time pads, codes and authentication systems and extracts as follows:

(1) (U) All **used key** must be destroyed immediately after supersession if possible, but no later than 12 hours after supersession. Local commanders, CONAUTHs, or other responsible officials may grant extensions up to a maximum of 72 hours on a case-by-case basis when fully justified. Except under combat conditions, extensions must be requested and approved, in writing, and retained on file with the Local Destruction Report for review by command inspectors and auditors.

(2) (U) It is not required that **unused** superseded daily or individual key settings be removed from secure storage for the sole purpose of destruction to fulfill the 12-hour destruction requirement (see paragraph 4.19.2 a [3] below). However, when individual key segments are removed from a canister for use, all previous unused segments that have become superseded will be destroyed within 12 hours. *ICP key will be destroyed IAW direction from the ICP manager.*

(3) (U) Notwithstanding item (2) above, **unused, superseded, keying material** must be destroyed not later than 5 days after the supersession date. Distribution accounts (CLSFs) are required to destroy unused superseded keying material not later than 15 days after supersession; however, more frequent destruction of such material is recommended.

**b. (U) Exception to COMSEC Account Destruction Procedures.**

(1) (U) Ten-day increments of CONFIDENTIAL DRYAD and OPCODES that are used with Signal Operating Instructions (SOI) for on-line operations will be destroyed immediately after supersession but no later than 12 hours afterward. Local commanders, CONAUTHs, or other responsible officials may grant an extension, in writing, of up to a maximum of 72 hours on a case-by-case basis (see subparagraph 4.19.a.2 [1] above).

(a) (U) The user will destroy this material. A witness is not necessary and a Destruction Report is not required (see paragraph 4.16.b).

(b) (U) Do not return DRYADS/ OPCODES material to the custodian or other persons who originally issued the key. Any unnecessary retention of material for administrative purposes increases the possibility of loss or compromise.

(2) (U) All superseded key, used or unused, which is held in facilities designated as high risk per AR 190-51 by cognizant security officials, will be destroyed immediately after supersession, if possible, but no later than 12 hours after the date the material is superseded, **without exception**. All operational COMSEC Facilities deployed outside the U.S., its possessions, and its territories are considered to be Mission Essential or Vulnerable Areas (MEVA).

**c. (U) Unused Key Marked "CRYPTO."** All key marked "CRYPTO" and held in Contingency or Reserve status will be superseded and destroyed IAW AR 380-40.

**d. (U) Maintenance and Sample Key.** Maintenance key and sample keying materials that are not designated "CRYPTO" are not regularly superseded. Such material should be destroyed only when it becomes physically unserviceable or is no longer required.

**e. (U) Other COMSEC Material.** Destroy all COMSEC material other than key (e.g., operating instructions, maintenance manuals) immediately after the item is superseded. The residue of amendments to COMSEC publications (e.g., KAMs, KAOs) must be

destroyed no later than 5 days after posting the amendment. Regardless of extenuating circumstances, which may justifiably cause short delays in destruction of this category of material, it must be destroyed no later than the 15th day after the date the item was superseded.

**f. (U) Allied Publications.** Destruction of Allied Publications by U.S. elements will be performed as directed by appropriate NATO and Allied Directives.

**4.19.3 (U) Destruction Procedures.** Except as noted in paragraph 4.19.2 b. above, destroy key in the presence of a cleared witness having a security clearance equal to or higher than the material being destroyed. The witness is required to participate in a joint inventory, to observe all key being destroyed, and to sign the appropriate disposition record. In unique situations when the operational instructions specifically state signature of a witness is waived, a witness is not required for the destruction of classified key. The lack of space on a Disposition Record for a witness signature or initials does not constitute a waiver.

**4.19.4. (U) Destruction of Paper-Based COMSEC Material and Keying Material, and of Mylar Key Tapes.** Destroy keying material by complete burning, or through use of approved pulverizing devices, wet pulping, disintegrators, or chemical alteration.

**(U) For physical destruction purposes, Keying material is divided into two categories: Paper keying material, and Key Tape. Key Tape will not be considered as paper. ALL key tape will be treated as non-paper (i.e., Mylar) material.**

**a. (U) *Burning.*** Burning is the preferred destruction method for all keying material. Burning methods and equipment used must have prior approval of the local command's physical security officer. During the burning process, make sure that combustion is complete and that all material is reduced to a white ash. When burning key material, the fire and appliances used to generate the fire must be within a contained area and controlled so that no unburned pieces are allowed to escape by fire-generated air drafts or wind currents. Inspect ashes and, if necessary, break up residue and re-burn or reduce to sludge by adding water.

**b. (U) Disintegrators.** Use of disintegrators (pulverizing machines, hammermills, or knifemills) for final destruction of paper-based COMSEC keying material is considered to meet the specifications of CNSS No.16, and may continue to be used for destruction of this material. These destruction devices may be used to perform final destruction for printed or punched key tape ONLY IF THE NSA has specifically approved the device, and/or by subsequent HQDA (G-2) documented and approved methods. COMSEC personnel must ensure the disintegrator machine has thoroughly reduced the material to bits or fibers that are too small to be reconstructed. Check the machine and its residue before and after each use. Materials that have been disintegrated in strict compliance with the policies contained in NCSS No. 16 and this TB are considered destroyed beyond reconstruction.

**c. (U) Double-cut Shredders.** Effective 1 January 2003, use of previously approved d*ouble-cut (crosscut) shredders* conforming to the standard defined in NTISSI No. 4004 (i.e., waste particle size of 1/2 " x 1/32") were no longer authorized for the terminal destruction of any paper-based COMSEC material, key, or otherwise.

(1) (U) In situations where burning, pulverization, or destruction of paper-based COMSEC material by use of an approved device is not feasible, old-specification crosscut shredders may continue to be used to destroy "non-CRYPTO-marked key" and other paper COMSEC material until the organization takes delivery of a new-specification crosscut shredder, or until 30 September 2003, whichever occurs first.

(2) (U) As of 1 October 2003, a new-specification crosscut shredder, or an approved alternate destruction process, is required for the destruction of all paper-based COMSEC material. The device must meet the new standards and specifications as defined in the NSA/CSS Evaluated Products List for High Security Crosscut Paper Shredders (NSA/CSS EPL-02-01, dated 1 August 2002, or later).

(3) (U) During the period 1 January to 30 September 2003, old-specification crosscut shredders may continue to be used on a temporary basis as a **"first step"** in the destruction process toward the final destruction of the material. This interim period has been granted to facilitate a smooth transition to the new method of destruction.

(4) (U) After 1 October 2003, when destroying COMSEC material marked "CRYPTO" (e.g., keying material or key tapes) the use of a crosscut shredder (old or new specification) **SHALL NOT** be considered as a "final" destruction method and **MUST** be augmented by additional precautions to ensure the final destruction of the material (see paragraphs a. and b. below). Use of a destruction device for the final destruction of Key Tapes (i.e., destruction not augmented by additional precautions) will only be authorized in NSA-approved disintegrators, by burning, or in approved Key Tape-specific Destruction Devices (KTDD). Units that do not have burn facilities, approved disintegrators, or an approved KTDD must comply with the following:

(a) (U) When employing a crosscut shredder as a first step for keying material destruction, some additional precautions are necessary to ensure final "terminal" destruction: **Shredded keying material must not be treated, handled or disposed of as unclassified waste or in any manner that would allow an adversary access to all portions of the shredded keys.**

(b) (U) Shredded key shall be retained and stored as collateral classified material for later secure return to a facility which can burn or pulverize the shredded residue.
As an alternative, it can be dispersed in a method that will prevent or preclude collection of all portions of a key segment. A common sense approach should be used to identify potential post-shredding destruction processes that will achieve this objective. For example, flushing mixed shredded residue down a toilet will prevent collection of all pieces for reconstruction, or dispersing it into the ocean will accomplish the same objective. As a last recourse, shredding amounts of keying materials, mixing with other shredded material, and loosely dispersing "by hand" in multiple and random trash containers will preclude a systematic collection and reconstruction of the residue.

(5) (U) *Wet Pulping.* Wet pulping devices may be used ONLY IF they reduce the paper to a state such as that no information can be recovered from the residue (i.e., no pieces larger than 5 mm [0.2 inches] in any dimension). To date, the only approved wet-pulping device is a good quality household blender. The blender will destroy a few sheets of low wet-strength paper at one time.

(6) (U) *Electro-Media Material.* Material in other than paper form (e.g., magnetic tape, microfiche, microfilm) must be burned, chopped, pulverized or chemically changed so that there is no possibility that information can be physically, electrically, optically, or otherwise reconstructed. Floppy disks will be destroyed IAW AR 380-19. Examples of preferred destruction methods for electro-media based non-paper key are as follows:

**SODIUM NITRATE: WARNING**

Do not incinerate magnetic tape on aluminum or magnesium alloy reels. Combustion of the reel could cause severe burns or eye damage!

(a) (U) Microforms (microfilm, microfiche, or other reduced image photo negatives) may be destroyed by burning or by chemical methods. An example of a chemical method is immersion of diazo reproductions in acetone or methylene chloride. Immersion must be for a 5-minute period or longer. Sheets must be separated and film must be unrolled.

(b) (U) Handle magnetic or electronic recording or storage media on an individual basis as follows:

- (U) Magnetic tape may be destroyed by disintegration or incineration.
- (U) Magnetic cores may be destroyed by incineration or by smelting.
- (U) Magnetic diskettes, disk packs, and drums may be destroyed by removing the entire recording surface using an emery wheel or disk sander or by smelting.

(c) (U) Compact Disks (CDs). The NSA has approved the use of the SEM Model 1200 CD-ROM Declassifier for secure routine declassification and destruction of both classified and unclassified compact disks. For more information, on the price and availability of this product, contact Security Engineered Machinery, Inc. in Westboro, MA. Telephone: (508) 366-1488.

(d) (U) Units that do not have this NSA-approved equipment must ship both classified and unclassified CD-ROMs containing sensitive COMSEC information to the NSA for destruction. For additional instructions on the shipment of CD-ROMs to the NSA, telephone (301) 688-5467.

(e) (U) Unwanted CDs that are unclassified and contain only non-sensitive information may be broken into pieces and placed in waste receptacles. CAUTION: Do not attempt to destroy CDs by burning; this media contains toxic substances that produce hazardous fumes harmful to humans.

(7) (U) *Extracts of Codes, Ciphers, and Authentication Systems.* **During actual combat operations**, you may destroy individual extracts of CONFIDENTIAL codes, ciphers and authentication systems by hand tearing into the smallest pieces possible and then dispersing over a wide area. Mylar tape (standard hole key tapes) will have to be cut into small pieces. The hand-tearing method is authorized only when burning or other destruction methods are not available.

**4.19.5 (U) Destruction of Other COMSEC Material.** Destroy paper material other than key (e.g., operating instructions, maintenance manuals) using the methods directed in the preceding paragraph, or by using destruction methods authorized in AR 380-5 for information of the same classification. Destroy non-paper material (e.g., microfiche, magnetic tape, floppy disks) as directed in paragraph 4.19.4.

**4.19.6 (U) Destruction of Accountable COMSEC Material on Hand Receipts.** For schedule of destruction see paragraph 4.19.2.

**a. (U) Record of Disposition of Key Material**. Destruction of keying material will be recorded on the Record of Disposition page for the appropriate key material. When all keying material in the book, canister, etc., has been destroyed, the Record of Disposition page will be returned to the issuing COMSEC Custodian as proof of destruction.

**b. (U) Documents Without Record of Disposition.**

(1) (U) When the COMSEC Custodian authorizes routine destruction of material not containing a Record of Disposition page, the Hand Receipt Holder may prepare a Destruction Report using the SF 153 (two copies) as shown in Figure 4-8 and Table 4-7. A signed copy will be forwarded to the COMSEC Custodian and the remaining copy retained on file by the Hand Receipt Holder. As an alternative to the SF 153, users may record destruction on DA Form 5941-E (Appendix D).

(2) (U) If the COMSEC material is the type that has to be destroyed on a daily basis, the COMSEC Custodian will normally provide a locally prepared Daily Destruction Certificate to the user. If the custodian does not provide one, the Hand Receipt Holder will prepare one. The local daily record of destruction can

be any form suitable to positively identify the material that is being destroyed. The Daily Destruction Certificates will be marked with the appropriate classification once the certificate has been filled in with classified information. Usually, the classification will be "CONFIDENTIAL"; however, the certificate will not be marked if the key tape is unclassified. When marked, the letters must be larger than the largest letters printed on the form IAW AR 380-5. The local record of daily destruction will be signed and returned to the COMSEC Custodian as proof that the material was destroyed.

## 4.20 AUDIT/INSPECTION OF COMSEC ACCOUNTS.

(U) Audits and COMSEC Facility Inspections are performed simultaneously by CSLA. Throughout the contents of this chapter, when the term "Audit" is used, it will be understood to include the Facility Inspection.

**4.20.1 (U) Basis for Audit.** The formal CSLA COMSEC Audit program is the Army method mandated by HQDA to certify and validate central accountability and the proper safeguarding and control of COMSEC Material. CSLA will conduct audits of Army COMSEC accounts under the provisions of AR 380-40, Chapter 6. Each audit by CSLA is conducted separately from local command inspections.

**4.20.2 (U) Notification of Audit.** When an audit is scheduled for a COMSEC account, prior notice will be sent 45 days in advance to the COMSEC account with a copy of the notification being furnished to the account's MACOM. Upon receipt of the audit notification, the account is required to acknowledge it has been notified of the impending visit. It is the COMSEC Custodian's responsibility to notify his/her higher headquarters of the upcoming audit. All accounts are subject to unannounced audit/inspection; however, an unannounced audit/inspection would only occur under unusual situations and would be coordinated through the MACOM of the affected account IAW AR 380-40, Chapter 6-3b.

**4.20.3 (U) Scope of the Audit.** A COMSEC audit will encompass all safeguarding, accounting and security procedures required by AR 380-40 and TB 380-41. The following is an overview, but it is not limited to what may be conducted during an audit. For a detailed listing of items that a COMSEC auditor will be reviewing, see Appendix G of this TB.

**a. (U)** Verify physical security measures are employed to ensure COMSEC material is properly safeguarded.

**b. (U)** Verify COMSEC Custodian, alternates and maintenance personnel are properly certified through an approved school-training program.

**c. (U)** Ensure access to the COMSEC Facility is being controlled and all security locking devices (X07s, X08s, X09s, cipher locks, etc.) are being properly maintained IAW AR 380-40 and this TB.

**d. (U)** Verify that combinations to all combination locking devices are changed on a regular basis IAW AR 380-5, and that all SF 700s and SF 702s are being maintained properly.

**e. (U)** Ensure OCONUS COMSEC Accounts have emergency plans completed and have been rehearsed IAW AR 380-40.

**f. (U)** Ensure that COMSEC Command inspections are being performed and that any corrective actions have been taken based upon the inspector's findings.

**g. (U)** Ensure Reportable and Administrative COMSEC Incidents are being filed and corrective actions to prevent further incidents are being employed.

**h. (U)** Ensure COMSEC accounts are storing, distributing, and destroying COMSEC key IAW AR 380-40 and this TB.

**i. (U)** Ensure completed physical inventories of COMSEC material charged to the account, including material on hand receipts, are being conducted.

**j. (U)** Verify completeness and accuracy of all accounting records and files.

**k. (U)** Prepare a Certification and Correction (C&C) page for the audit inventory. The C&C page will be prepared and signed by the COMSEC Custodian and CSLA Auditor at the conclusion of the audit. The Audit Inventory Report will serve as the SAIR. "Additions" and "Deletions" to the C&C page of the Audit Inventory Report will include all transactions that have occurred as of the date of the signatures on the C&C page.

**l. (U)** Solicit the COMSEC Custodian's accounting problems and recommendations.

**m. (U)** Provide auditor's recommendations for improvement of local accounting procedures.

**n. (U)** Provide exit briefing for the commander of the COMSEC account to ensure the commander is aware of the condition of his/her COMSEC account.

**4.20.4 (U) Suggested Local Pre-Inspection Checklist.** To assist the COMSEC Custodian in preparing for an Audit and Facility Inspection, a checklist is provided in Appendix G.

**4.20.5 (U) Audit Report.**

**a. (U)** Upon completion of an audit, any situation requiring immediate action will be brought to the attention of the COMSEC Custodian and the unit commander, or the commander's representative, at the exit briefing.

**b. (U)** A formal Audit Report outlining the condition of the COMSEC account and recommended improvements will be forwarded directly to the commander of the audited COMSEC account (ATTN: To the Commander) within 30 days following the visit. The Audit Report will list discrepancies found, general observations and recommendations, and the overall rating of the account. A copy of the report will be provided to the higher headquarters in the unit's chain of command responsible for the Command COMSEC Inspection Program mandated by AR 380-40. It is the unit commander's responsibility to apprise intermediate levels of command as to the results of the audit.

**c. (U) Audit Rating.** Upon completion of an audit, a rating will be assigned to summarize the condition and status of a COMSEC account based on facts and circumstances, as perceived by the auditor. This rating is based strictly on regulatory standards without distortion by personal feelings, prejudices, or interpretation. The rating is designed to reflect the true condition of the COMSEC account to the commander and is not necessarily a reflection of the current COMSEC Custodian. In many instances, the custodian may have only recently assumed responsibility for the account and the discrepancies found are attributable to a prior custodian. However, when an incoming custodian signs for the account, that person assumes full responsibility for the account, the COMSEC Facility and all account records in their current condition; therefore, a new custodian must ensure all discrepancies are corrected before the old custodian is relieved. Accounts will be rated as **Satisfactory, Marginal,** or **Unsatisfactory** based on the auditor's evaluation of all factors.

(1) (U) A SATISFACTORY rating indicates the auditor found both the security and accountability of the COMSEC material to be acceptable even though minor discrepancies may exist.

(2) (U) A MARGINAL rating is when:

(a) (U) The auditor finds numerous repetitive deficiencies of a minor administrative nature, which do not directly impair the accountability or security of the material; however, they do reflect a failure on the part of the custodian (past or present custodian) to pay sufficient attention to detail and would indicate a potential for more serious problems in the future.

(b) (U) An administrative type of incident as described in AR 380-40, paragraph 7-3d is discovered. However, if an account has multiple administrative incidents, the account may receive an UNSATISFACTORY rating.

(3) (U) An UNSATISFACTORY rating indicates the auditor found serious problems, such as the possible loss of accountability of COMSEC material, or several deficiencies that directly impair accountability or security of the material in the account. The following are

examples of serious deficiencies, but they are not all inclusive:

(a) (U) An unreported COMSEC Incident involving loss of accountability.

(b) (U) Failure of the custodian to submit necessary accounting records to the COR.

(c) (U) Missing records for COMSEC material to local destruction documentation to support consolidated destruction reports.

(d) (U) Unauthorized locking devices or containers to secure classified COMSEC material.

(e) (U) Failure to comply with TPI procedures for TS material.

(f) (U) Discovery that discrepancies listed on a prior audit report, with an official written reply of resolution were, in fact, not resolved.

**d. (U) Command Action.** Upon receipt of the COMSEC Audit Report, the commander for whom the account is maintained will direct appropriate remedial action to resolve all deficiencies. Not later than 30 days following receipt of the formal report (no exceptions for Reserves and National Guard), a reply by endorsement signed by the commander will be submitted through command channels to CSLA detailing action taken. The higher command level responsible for the Command COMSEC Inspection Program mandated by AR 380-40 will review actions taken by the unit for adequacy, as well as take whatever follow-up action is deemed appropriate. In a case where an item has been lost, the auditor will either list the item as a "Deletion" and in the Remarks Column will annotate "Incident, date time group of the message or case number of the incident," or the auditor will list the material after "Nothing Follows" on the Certification and Correction Page. However, CSLA will not remove the item from the COMSEC account assets until the Army Service Authority has granted a "Relief from Accountability." CSLA will process and provide a Certification of Verification if no other discrepancies are discovered.

**THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY**

# CHAPTER 5

# SAFEGUARDING COMSEC MATERIAL

## 5.1 GENERAL.

(U) This chapter provides minimum standards for the protection and physical control of COMSEC material. To effectively safeguard and establish security for COMSEC material, it is vital that each COMSEC Custodian and assigned alternate custodian becomes familiar with and thoroughly understands the procedures, responsibilities and communications channels presented in this chapter.

## 5.2 CLASSIFICATION GUIDELINES FOR COMSEC INFORMATION.

(U) The following guidelines provide limited instructions on classifying COMSEC information. Additional guidance on classifying information pertaining to COMSEC equipment is contained in AR 380-40.

**5.2.1 (U) Foreign Release.** COMSEC information in any form is not releasable to foreign nationals unless specifically authorized. Requests for release will be forwarded to HQDA DCS, G-2 (ATTN: DAMI-CD) per AR 380-40.

**5.2.2 (U) Handling and Release of Unclassified COMSEC Information.** As a general rule, all unclassified COMSEC information is intended FOR OFFICIAL USE ONLY and should be withheld from public disclosure based on exemptions authorized under the Freedom of Information Act (FOIA). The open or public display of U.S. Government or foreign COMSEC material and information at commercial or other public meetings, open houses, or for other nonofficial purposes is forbidden unless specifically authorized by other HQDA Directives (see DA Pamphlet 25-380-2 for CCI). This prohibition includes discussion, publication, or presentation of COMSEC information for other than official purposes. Any requests for public or nonofficial display or publication of COMSEC information, including Freedom of Information Act (FOIA) Requests, will be referred to HQDA (DAMI-CD).

**5.2.3 (U) FOR OFFICIAL USE ONLY (FOUO) Application.** The protective marking FOUO will be applied to unclassified COMSEC information when the originator determines that it should not be publicly released. The marking will be based on the FOIA policies contained in IAW AR 25-55. As a minimum, the FOUO marking should be applied to the following types of information, if unclassified:

**a. (U)** Lists of COMSEC short/long titles.

**b. (U)** Narrative information on characteristics of COMSEC equipment.

**c. (U)** Indications of new COMSEC developments.

**d. (U)** COMSEC planning, programming, and budgeting information.

**e. (U)** Specifications and purchase descriptions pertaining to COMSEC equipment or the support of unique COMSEC requirements.

**f. (U)** Operating instructions, maintenance manuals, and publications related to auxiliary equipment developed exclusively for use with COMSEC equipment.

**g. (U)** COMSEC material reports (SF 153).

**h. (U)** Official photographs or line drawings of classified COMSEC equipment.

**i. (U)** Information of substance that relates to the application of cryptographic transmission or emission security measures to COMSEC information.

**5.2.4 (U) Compilations.** Compilation of unclassified COMSEC information may warrant classification (see AR 380-40, Appendix B).

**5.2.5 (U) Use of Caveat "CRYPTO."** The caveat "CRYPTO" is always capitalized and is defined as "The marking or designator identifying all COMSEC key used to protect or authenticate telecommunications carrying classified national security information and sensitive, unclassified Government or Government-derived information, the loss of which could adversely affect national security interests." The purpose of this marking is to identify only that key which must be handled and controlled under the special access, storage, distribution, accounting, and destruction requirement of the CMCS as set forth in this TB. The following apply:

**a. (U)** Key will be marked “CRYPTO” when its purpose is to authenticate a communication or provide protection against Signals Intelligence (SIGINT) exploitation and the communication will be passed by radio, microwave, cable (other than a protected distribution system), or other potentially exploitable means. Key, which does not meet these criteria, will not be marked “CRYPTO.”

**b. (U)** Most hard copy key produced by the NSA will be marked “CRYPTO.” The principal exceptions will be key intended for demonstration purposes, sample key for use in or outside the classroom, and maintenance key used exclusively for bench testing purposes. All other classes of key are intended to protect or authenticate and will be marked “CRYPTO.”

**c. (U)** The marking “CRYPTO” may be used on both classified and unclassified key (hard copy or software); it will not be used on equipment, manuals or other COMSEC material. **All AKMS-generated electronic key** will be understood to carry the “CRYPTO” designation and be protected accordingly.

**d. (U)** Key used to protect classified communications will be marked with the appropriate classification. Key used to protect unclassified national security-related telecommunications will not be classified unless the format or composition of the key is, in itself, classified.

**e. (U)** All physical key marked “CRYPTO” must be produced by the NSA and obtained through COMSEC logistics channels.

**f. (U)** The marking “CRYPTO” imposes no additional investigative or access requirements on U.S. personnel. A security clearance is not required for access to key marked “CRYPTO” if it does not bear a classification marking.

**g. (U)** Unclassified key marked “CRYPTO” will be stored in the most secure manner available to the user. As a minimum, it will be stored in a manner that is sufficient to preclude any reasonable chance of theft or access by unauthorized persons. It should be double-wrapped for shipment. It should be transmitted via the same means as classified key or, as a minimum, via U.S. Registered Mail. Upon receipt, packages should be examined and processed from a physical security standpoint in the same manner as classified key.

**5.2.6 (U) Marking of COMSEC Equipment.** COMSEC equipment and components in the U.S. inventory will carry markings as follows:

**a. (U) COMSEC Equipment and Assemblies**. All COMSEC equipment and assemblies (including telecommunications equipment with integral cryptography) will be marked with a short title, the term "GOVERNMENT PROPERTY," and the accounting number (serial number).

**b. (U) Element Boards**. Printed circuit element boards used in COMSEC equipment or performing COMSEC functions in other equipment will be marked with a short title and accounting number (serial number).

**c. (U) Other Items**. Those separate items, which perform a COMSEC function as determined by the NSA, will be marked with a short title.

**d. (U) Equipment and Assembly Short Titles**. With regard to the short titles mentioned in the preceding paragraphs:

(1) (U) Radio sets and other communications equipment with an integral COMSEC capability may, with the approval of the NSA, be nomenclatured in the Joint Electronic

Type Designation System (JETDS), MIL-STD-196D.

(2) (U) Short titles for COMSEC items will be assigned by the NSA.

**e. (U) Classified Items.** In addition, those items determined as classified by the NSA will bear an appropriate classification marking. COMSEC equipment with hardwired operational keying variables installed will be marked "CRYPTO."

**f. (U) Unclassified items designated CCI.** Unclassified CCI items will contain a CCI label (see paragraph 5.2.7).

**g. (U) Previous Markings.** Equipment marked under previous guidance need not be re-marked except as directed by the NSA.

**5.2.7 (U) Controlled Cryptographic Items (CCI).**

**a. (U)** CCI equipment is unclassified controlled end items or assemblies that perform a critical COMSEC or COMSEC ancillary function. Although CCI equipment is unclassified, it requires access controls and physical protection against actions that could affect its continued integrity. Physical protection controls applied to CCI are detailed in DA PAM 25-380-2.

**b. (U)** The marking "CONTROLLED CRYPTOGRAPHIC ITEM" or "CCI" will be used to identify those items of COMSEC hardware and microcircuits to the end item and assembly level when they are designated Controlled Cryptographic Items by the NSA.

**c. (U)** As a minimum, un-keyed CCI will be safeguarded as sensitive, valuable property. No security clearance is required for access to un-keyed CCI, but access will be limited per DA Pam 25-380-2 on a need-to-know basis. Sensitive Item management and controls, as prescribed in AR 710-2, will be applied to CCI.

**5.2.8 (U) COMSEC Classification Guidance.**

(U) See AR 380-40.

**5.2.9 (U) Classification Duration.** Cryptographic systems protect the most highly classified communications of the U.S. Government and its allies. COMSEC information must be protected to prevent hostile activities from building a database to exploit our systems, equipment, and material. Unless a particular item of COMSEC information will become declassified at a particular time or following a specified event, the item classification will be derived from the source document and the information shall be marked IAW DoD 5200.1-PH:

**Derived From:**
**Declassify On:**
**Date of Source:**

(U) In those instances where documents are prepared from multiple sources, the declassification date or event that provides the longest period of classification shall be used and entered in the “Declassify On” statement.

## 5.3 PHYSICAL SECURITY MEASURES.

**a. (U)** COMSEC material plays a vital role in the protection of national security communications. This chapter describes minimum physical security measures designed to safeguard the integrity of COMSEC material and the facilities in which COMSEC material is operated or stored. Access is defined as the capability and opportunity to obtain knowledge of or to alter information on material.

**b. (U)** The broad dispersal of COMSEC material and its positioning in a large variety of environments have created the need for increased emphasis on physical security procedures. Individual commanders are responsible for ensuring that access to classified COMSEC material within their commands or organizations is properly controlled and that the material is stored, accounted for, transmitted, and destroyed IAW AR 380-40 and this TB.

**c. (U)** The procedures for safeguarding COMSEC Material and facilities are designed to ensure the integrity of COMSEC material against the following threats:

(1) (U) Loss, theft, sabotage, unauthorized access to, or observation of COMSEC material.

(2) (U) Tampering with, or TEMPEST exploitation of, COMSEC material.

(3) (U) Clandestine exploitation of sensitive communications within a secure telecommunications facility.

**d. (U)** Users should also refer to local operating instructions for security procedures pertaining to specific systems, and to AR 380-40 for policy related to the security of COMSEC material. Security procedures for CCI are contained in DA Pam 25-380-2.

## 5.4 ACCESS TO AND IDENTIFICATION OF A COMSEC FACILITY.

(U) A COMSEC Facility is defined as a secure space, area, room, structure or series of structures approved by a competent authority for the primary purpose of generating, operating, storing, repairing or training personnel in the use or maintenance of classified COMSEC material. In those instances when, due to operational necessity, a larger facility is not required, a COMSEC Facility may consist of nothing more than a GSA-approved security container or multiple containers in a common administrative office area: provided adequate safeguards are present to inhibit unsupervised access by unauthorized individuals.

**a. (U) Access.** Access to COMSEC Facilities may be granted by the commander (or his/her designated representative) to personnel whose duties require such access (need-to-know). These personnel must possess security clearances equal to the classification level of the COMSEC material (as well as the national security information) to which they will have access. Commanders are authorized to employ local systems (e.g., clearance status rosters) for verifying individual clearances. Access is defined as the capability and opportunity to obtain knowledge of or to alter information or material.

**b. (U) Visitors.** Persons whose duties do not require access, or those who are not properly cleared, will be permitted entry only upon approval from the commander or his/her designated representative.

**c. (U) Visitors' Register.** DA Form 1999-E, Restricted Area Visitor Register, will be used to record the arrival and departure of any person not on the access roster. The commander may waive this requirement when the COMSEC Facility is merely a classified container (e.g., Mosler safe) within a common use office area. It is also at the discretion of the commander whether or not a visitor is/is not required to fill in the SSN block of the DA Form 1999-E. *The SSN, which is sensitive in nature and should not be openly displayed for public view, is already listed on the security clearance information form provided to the security manager of the restricted area prior to the visit.* (See Appendix D for reproducible forms.)

**d. (U) Privacy Act Statement.** Within COMSEC Facilities that the commander has determined the SSN will be used (i.e., an individual entering both his/her SSN and signature on the DA Form 1999-E), the following Privacy Act Statement, which appears at the bottom of DA Form 1999-E, *must* be conspicuous to the signer's view: "Authority: 10 USC 3012/EO. The SSN is used only for identification. Access to this COMSEC Facility may be denied without SSN."

**e. (U) Equipment Screening.** Except for closed crypto-equipment, all classified COMSEC material will be screened from view by visitors.

**f. (U) Visitor Surveillance.** All visitors will be kept under constant surveillance and will not be permitted access to classified COMSEC information.

**g. (U) Maintenance Personnel Access.** Maintenance personnel will only be allowed access to classified COMSEC equipment and information for which they have appropriate clearance. If maintenance personnel do not have the appropriate clearance, they MUST be kept under constant surveillance to prevent their unauthorized access to classified equipment.

**h. (U) Identification of Facility.**

(1) (U) In accordance with AR 190-13, Chapter 6, COMSEC Facilities SHALL be designated by the Installation/Activity Commander (or civilian equivalent), **in writing**, as a **RESTRICTED AREA.** A prominent sign placed conspicuously (bilingual where appropriate), and the

Warning Notice contained in paragraph 6-4, AR 190-11 will be posted to identify the restricted area. No other phrase will be used. Commanders outside the U.S., its possessions, and its territories will establish such restricted areas for COMSEC Facilities consistent with local security conditions, risk assessments, and Host-Country Agreements, as applicable.

(2) (U) When conditions warrant, the designation of a COMSEC Facility as a Restricted Area may be waived, at the commander's discretion. For example, when a COMSEC Facility is merely a safe or series of classified containers within a common use office area or building, the designation of that limited space occupied by the classified container(s) as a "Restricted Area" may not be appropriate.

(3) (U) To enhance security, the physical location of a COMSEC Facility will not be advertised or made conspicuous by the posting of external signs, except as noted above for the placement of a "Restricted Area" sign. However, within a secure or restricted area that is not accessible to the general public, there are no restrictions as to the placement of "internal signs" giving directions to a COMSEC Facility or identifying a room or office as the COMSEC Facility for the benefit of customers and other official visitors to the COMSEC Facility.

## 5.5 PROTECTION OF FIXED COMSEC FACILITIES.

(U) Fixed COMSEC Facilities are vulnerable to both overt and covert security violations. Standards for securing and protecting fixed COMSEC Facilities are presented in this paragraph and are the minimum-security measures that must be employed.

**5.5.1 (U) Installation of On-Line Crypto-Equipment.** To prevent foreign intelligence exploration of compromising emanations, the installation of on-line crypto-equipment and supporting communications equipment in COMSEC Facilities will be directed by NSTISSAM TEMPEST/2-95. For additional guidance see your Certified TEMPEST Technical Authority (CTTA).

**5.5.2 (U) Secure Room Operations.** When fixed plant COMSEC Facilities employ several types of COMSEC equipment and handle a large volume of classified traffic, the facility will be located in a SECURE ROOM or CONTROLLED AREA as specified in the following paragraphs:

**a. (U) General Office Use.** When the COMSEC Facility area is also used for general office purposes, it is the responsibility of the commander to enforce compliance with access requirements as described in AR 380-40. CCI equipment keyed with unclassified “CRYPTO” key used for passing Sensitive But Unclassified (SBU) information will be provided double barrier protection.

**b. (U) Secure Storage Area**. If a COMSEC Facility is used for secure storage of classified material, facility construction standards apply as directed by AR 380-40.

**5.5.3 (U) General Area Operations.**

(U) When fixed COMSEC Facilities do not have the requirements for a signal center, they may be located in a controlled, general area.

**5.5.4 (U) Devices (other than COMSEC Equipment) Used Within a COMSEC Facility.** Communication devices, such as telephones, interoffice communication systems and other transmitting devices, must meet the provisions of AR 381-14 (C) when installed in an operational COMSEC Facility. This restriction does not apply to a COMSEC Facility used solely for storage of COMSEC information. For all other items, see AR 380-40.

**5.5.5 (U) Electronic Access Control Devices.** Electronic access control devices (e.g., cipher locks, keyless push buttons) do not afford the required protection against unauthorized admittance and, therefore, will not be substituted for the required built-in, three-position combination lock.

**a.** (U) Electronic access control devices will be properly installed to prevent tampering. Electronic access control devices using electro-mechanical locks may be used in addition to the built-in, three-position combination lock. In this case, the electronic access control devices will

be used only for the admittance of known authorized personnel into occupied or otherwise guarded COMSEC Facility areas.

**b.** (U) Operation of electronic access control devices will meet the following criteria:

**c.** (U) The code sequence will be screened or masked to prevent unauthorized viewing during door-opening procedures.

**d.** (U) A positive means will be provided to ensure identification of all persons prior to their admittance.

**e.** (U) Authorized personnel will change code combinations annually, upon duty termination of any individual who knows or has access to the code combination, and at any time the code becomes compromised. An SF 700 will be used to record combination change information and will be posted to the inside of the door.

**f.** (U) Push buttons will be kept dust free to prevent reconstruction of the code.

## 5.6 SECURITY CHECKS.

(U) Security checks will be made by COMSEC Facility personnel or by other specifically designated personnel.

### 5.6.1 (U) Types of Security Checks.

**a. (U) End of Workday Security Check.** As directed by AR 380-5, at the end of each workday, Security Container Check Sheet (SF 702) will be used to verify that each security container, cabinet, secure room, or vault containing classified material is secure. When another individual is not present to check the locks for security, the person who locked the container, cabinet, room or vault must also perform the second security check and complete the "checked by" section of the SF 702. Such checks must be performed as a separately distinct action after the locking process to satisfy the requirements of AR 380-5.

**b. (U) Non-Workday Security Check.** Non-workday Security Checks are not required unless the facility is opened during weekends, holidays, or after hours. If the facility is a TS facility located in OCONUS, a non-workday Security Check ***IS*** required unless an Intrusion Detection System is operating.

**c. (U) 24-Hour Operations.** In a COMSEC Facility that operates continuously (24-hours-a-day), an area check will be completed at the end of each shift and the SF 702 properly annotated IAW AR 380-5.

### 5.6.2 (U) Area Security.

**a. (U) Non-continuous Operations.** COMSEC Facilities, which do not operate continuously, require a security check be made at the end of each workday to establish that the facility is secure and that all classified COMSEC information is properly stored and safeguarded.

**b. (U) Area Checklist.** Area checklist forms will be designed and produced by the local commander (an SF 701 may be used). The area checklist will provide for and require the signature or initial of the individual performing the check. The area checklist will verify that:

(1) (U) Security containers are locked and double-checked.

(2) (U) Classified trash is properly stored.

(3) (U) Windows are locked.

(4) (U) Alarms are activated and working properly.

(5) (U) Other security measures are in effect IAW local SOP.

## 5.7 PROTECTION OF MOBILE AND TRANSPORTABLE COMSEC FACILITIES.

(U) The requirements for safeguarding mobile or fixed COMSEC Facilities are basically the same. Mobile facilities require that security measures be adapted to the particular environment of the operation. Un-keyed COMSEC equipment, which is installed in ground/air/water vehicles, should not be removed for storage provided they are protected to a degree which, in the judgment of the commander or responsible authority, is

sufficient to preclude any reasonable chance of theft, sabotage, tampering or access by unauthorized persons.

**5.7.1 (U) Protection.** During CRYPTO-operations, guards will protect all transportable and mobile COMSEC Facilities. Operating personnel satisfy the requirement for guards when the facility layout and operator duties make it feasible for operators to provide adequate control.

**5.7.2 (U) Minimum Mobile COMSEC Facility Protection.** As a minimum, protection for mobile COMSEC Facilities will be provided by one of the following methods:

**a. (U) Full-Time Guards.** Full-time guards will be stationed within sight of the COMSEC Facility if there is no supplemental protection, or if there is a possibility of unauthorized removal of the vehicle.

**b. (U) Patrol or Guard Post.** A patrol or a guard post may be used providing it is supplemented by an alarm system having a response time of five minutes or less. This security system must be implemented so that there is no possibility of unauthorized removal of the vehicle.

**c. (U) Guards Stationed at Entrances to a Fenced Area.** Guards can be stationed at all entrances to a fenced, restricted area (such as a protected, fenced motor pool). In this case, access must be restricted to properly cleared and authorized individuals.

## 5.8 USE OF GUARDS.

**a. (U) Clearance Requirements.** Guards who have ACCESS to classified COMSEC material must be properly cleared to the highest level of material held. ACCESS is defined as the capability and opportunity to obtain knowledge of or to alter information or material. Guards with area control duties only (e.g., motor pools, buildings) need not be cleared when they are used to support other security measures and will not normally have access to classified information.

**b. (U) Determination of Access.**

(1) (U) The commander will determine whether guard personnel (including foreign nationals) guarding flight lines, aircraft, motor pools, or vehicles are providing area control or will also have access to the COMSEC equipment installed therein. Foreign nationals will not have unescorted access to COMSEC equipment. If, in the judgment of the commander, supporting supplementary measures (e.g., locked aircraft and vehicles, fences) provide adequate protection to prevent any reasonable possibility of access to the COMSEC equipment by the guards, the guards will be considered to be providing AREA CONTROL.

(2) (U) Guards who are not given access to COMSEC material, and who are used to supplement existing physical security measures, need not meet access requirements. If a facility is located in U.S. or Allied territory, a roving guard who makes rounds at least every four hours is sufficient as long as the COMSEC material is appropriately secured. In Allied countries, guards employed by the host country may be used for area control.

(3) (U) If a facility is located in non-U.S., non-Allied territory, U.S. guards must be used and they must be situated at all times in the immediate area of the facility, preferably within the facility.

**c. (U) The Use of Un-cleared Guards.** Normally, properly cleared guards will be used to secure a COMSEC Facility. However, the clearance of guards protecting closed vehicles or shelters, which serve as COMSEC Facilities, may be waived provided:

(1) (U) The COMSEC Facility enclosure is constructed to positively prevent undetected access.

(2) (U) The main entrance to the COMSEC Facility is secured by a Group 1R combination-locking device. When this is not possible, the main entrance will be secured with an approved high security padlock.

(3) (U) The facility entrance is constructed or arranged to prevent viewing of COMSEC material when the door is open.

(4) (U) All entrances other than the main entrance to the COMSEC Facility are bolted with panic hardware (emergency mechanisms that open only from the inside).

(5) (U) Door hinges are installed in a manner to positively prevent unhinging of the door from the outside.

(6) (U) All windows within the facility are barred and securely fastened from the inside. Windows will also be screened to prevent unauthorized viewing from the outside.

## 5.9 EMPLOYMENT OF COMSEC EQUIPMENT AT UNATTENDED SITES.

(U) Special situations may require that certain COMSEC equipment be located at unattended sites. This practice may be authorized, but will be subject to the following safeguards:

**a. (U) Unattended COMSEC Equipment Storage**. As a general rule, uninstalled, classified COMSEC equipment and COMSEC maintenance manuals are not authorized to be stored at unattended sites. However, when mission priorities dictate, one on-line spare may be installed at the commander's discretion to provide redundancy for operational circuits, provided special security measures as prescribed in paragraph 5.10.3c are employed. In addition, COMSEC equipment loaded with classified key must be secured in an GSA-approved security container or equipped with locking bars secured by an approved, high security, combination padlock (NSN 5340-00-285-6523) meeting Federal Specification FF-C-110. CCI equipment keyed with unclassified "CRYPTO" key used for passing SBU information will be provided double barrier protection.

**b. (U) U.S. Unattended Site**. Adequate U.S. or Allied military forces must be located in the vicinity of any unattended site. This reaction force must be adequate and able to respond to an alarm within 15 minutes to minimize the possibility of enemy capture or temporary occupation of the site. The commander responsible for operation of the unattended site will need to arrange for an immediate guard force to respond in emergencies, and the appointment of an AR 15-6 board (when appropriate) who is responsible for investigating incidents involving threats to the COMSEC equipment on the site. Commanders must comply with the requirements of AR 380-5, AR 190-16, DA Pamphlet 25-380-2, and paragraph 5.10 of this TB.

**c. (U) Unattended Cryptonets**. Cryptonets whose key is held in COMSEC equipment located at unattended sites will be kept as small as possible. Unique key will be used on each link terminated at an unattended site.

**d. (U) Unattended Key Storage**. Key other than that electronically or physically held in the COMSEC equipment **will not** be stored at an unattended site.

**e. (U) Site Inspections**. Unattended sites will be periodically inspected at random intervals (as determined by the commander) to verify that no one has tampered with the COMSEC equipment. Site inspections will be performed at a minimum of once a month.

## 5.10 STORAGE OF COMSEC MATERIAL.

(U) Storage means the use of security containers, vaults, alarms, guards, and so forth, to protect COMSEC material or information when it is not under the direct and continuous control of properly cleared and authorized personnel. In contrast, when classified COMSEC material is in use by, in the physical possession of, or continuously attended by properly cleared personnel, its protection is presumed. For guidance on PCM, refer to CJCSI 3260.01.

**5.10.1 (U) Storage of Classified "CRYPTO" Key.** Classified key marked "CRYPTO" will be stored by one of the following methods in accordance with its classification:

**a. (U) TOP SECRET.** TOP SECRET key will be stored in a dual safe (safe stored inside a safe) with each compartment having a different, approved, combination lock IAW AR 380-40; or a GSA-approved safe with an electro-mechanical, dual digit (two combination) lock meeting Federal Specification FF-CC-2740 (X07/X08). Two SF 700s, prepared and stored separately, are needed to record the two combinations required for a TS storage container to ensure TPI for TS material is established and maintained. See AR 380-40, paragraph 2-18d for further information.

(1) (U) Store in any GSA-approved safe-type container that has not been altered through unauthorized modification.

(2) (U) Store in a vault constructed as directed in AR 380-40.

(3) (U) Alarmed Area. The TS storage area will be securely constructed and have substantial barriers to prevent unauthorized or forced entry. Barriers will be constructed so that forced entry will leave evidence of such entry and trigger an alarm or alert a guard.

**b. (U) SECRET.**

(1) (U) Store SECRET key by any one of the methods designated for TOP SECRET key.

(2) (U) Store in a GSA-approved storage container, which has a built-in, three-position, dial-type combination lock.

**c. (U) CONFIDENTIAL.**

(1) (U) Store CONFIDENTIAL key by any of the methods designated for TOP SECRET or SECRET key identified in the preceding paragraphs.

(2) (U) Store in a steel file cabinet. The file cabinet will have a built-in, changeable, three-position combination lock.

**5.10.2 (U) Storage of Unclassified "CRYPTO" Key.** Unclassified CRYPTO key will be stored using the same methods used for classified key, if practical, or in the most secure method available to the user. As a minimum, unclassified CRYPTO key will be stored in a manner that will provide security against the possibility of theft or access by unauthorized persons.

**5.10.3 Storage Restrictions.**

**a. (U) Mobile Storage.** In mobile or transportable facilities wherein normal storage means are not practical, only limited amounts of essential keying material may be stored. The following procedures apply:

(1) (U) The applicable requirements of paragraph 5.7apply.

(2) (U) Security containers must be securely affixed to the facility.

(3) (U) COMSEC holdings will be limited to those that are operationally essential to perform the mission. No more than a single edition of keying material will be held.

(4) (U) Unattended facilities, which contain keying material or keyed COMSEC equipment, will be guarded by appropriately cleared U.S. personnel. Commanders will comply with the contents of AR 190-16 and paragraph 5.9 of this TB.

**b. (U) Storage Containers.**

(1) (U) Older Security Containers. Security containers that were previously approved, but do not meet current standards, may continue to be used (with written CSLA approval) until approved containers can be obtained through normal supply channels.

(2) (U) Repair of Damaged Security Containers. In the event of restoration or repair, the security integrity of containers must be restored IAW the standards specified in AR 380-5. Containers that have been repaired or restored to meet original security specifications may be used to secure classified COMSEC information (except for TOP SECRET COMSEC keying material and information).

(3) (U) Non-approved Containers. Non-approved security containers will be

protected by continuous guard or by an alarm system. When using an alarm system, frequent irregular security checks will be made of the area.

**c. (U) Supplementary Control Methods.** During storage, vaults, alarmed areas and security containers that contain classified CRYPTO key must not be accessible to unauthorized personnel.

(1) (U) To prevent accessibility, supplementary control methods will be used. For example:

Locked rooms.
Locked and guarded buildings.
Alarms.

(2) (U) For each security situation, commanders must determine what supplementary controls are necessary to prevent unauthorized access to the storage device. Normally, guards or security forces used under these conditions need not be cleared. Refer to paragraph 5.8.a for further information.

**5.10.4 (U) Storage of COMSEC Equipment and Components.**

**a. (U) Non-Operational Configurations.** When classified COMSEC equipment or components are not installed in an operational configuration, such items will be stored in the same manner prescribed for material of the same classification as directed by AR 380-40.

(1) (U) Unclassified equipment and components other than CCI will be stored by a suitable method which will prevent any reasonable possibility of theft, sabotage, tampering, or access by unauthorized persons.

(2) (U) CCI (keyed or un-keyed) shall not be stored in vaults, security containers, or arms storage facilities containing items of monetary value (e.g., cash, jewelry, precious metals, etc), weapons, ammunition, or other sensitive items. Commanders must recognize that each additional item of value stored in a single security storage facility increases the risk of loss by intensifying the target potential to criminal and subversive elements. However, under emergency or tactical contingency conditions, when other secure storage facilities are not reasonably available, commanders may authorize short-term storage (not to exceed 30 days) of CCI in a consolidated secure storage facility. Long term storage of CCI under these conditions must be supported by a formal risk assessment per AR 190-51, and the authorization provided, in writing, to the Accountable Officer by a commander of grade 05 or above in the chain-of-command. See DA PAM 25-380-2 for further information on storage of CCI.

(3) (U) CCI, common fill devices and uninstalled COMSEC equipment will not be stored keyed except when specifically authorized in the system operating instructions or by other competent authority.

**b. (U) Operational Configurations.**

(1) (U) When un-keyed classified COMSEC equipment is installed in an operational configuration in a ship, aircraft, vehicle, building, etc., it may be left unattended provided it is otherwise protected to a degree which, in the judgment of the commander, is sufficient to prevent the likelihood of theft, sabotage, tampering or access by unauthorized persons. Installed COMSEC equipment will not be removed from vehicles for the sole purpose of providing security storage. Frequent removal of COMSEC equipment and subsequent reinstallation can cause equipment failure and downgrade operational readiness. When the installed COMSEC equipment is keyed, provisions of AR 380-40 and AR 380-5 apply.

(2) (U) Normally, the same protection provided for vehicles, or high value and government property, is adequate for the protection of un-keyed unclassified COMSEC equipment installed in vehicles and facilities. The responsible commander will consider the sensitivity, value of the equipment, and other factors (such as environment) when

determining acceptable security requirements and methods for protecting un-keyed, unclassified COMSEC equipment.

(3) (U) A tactical vehicle parked in a public location is not adequately protected unless physically attended or under the visual control of a responsible person. Such basic protection measures are even more essential when a vehicle is equipped with a radio and COMSEC equipment is installed in the vehicle. In addition to the protection provided to COMSEC equipment when un-keyed, enhanced protection must be provided to keyed equipment to prevent its unauthorized use or the unauthorized extraction of its key.

**c. (U) Special Cabinets for COMSEC Equipment.** The NSA has approved the use of special cabinets for COMSEC equipment in operational configurations. These cabinets do not have NSNs and are not manufactured under a GSA contract. They are available from their sole source manufacturer, the Mosler Safe Company. No other vendor has offered similar special-purpose crypto-equipment safes for government procurement. Because of limited projected use, these security cabinets will not be submitted to GSA for certification. Since these cabinets deviate from federal specifications, they do not bear the GSA label. As a result, the containers are not authorized for storage of superseded or future key. However, these cabinets may be used to store equipment containing the current key. Direct all orders and inquiries to:

Mosler, Government Sales
8509 Berk Blvd.
Hamilton, OH 45015-2213
(Telephone 1-800-568-7233)

**d. (U) Approved Modified Special Cabinets.** The following modified security cabinets are approved for closed-door operation and storage of COMSEC equipment.

(1) (U) Mosler Model 54-40 Special Class 5 Double Door Security Cabinet. This cabinet is designed for closed-door operation. It contains fans and secured vents and is provided with three holes in the top for power conduit mounting. The inside clear dimensions are H 48 1/2" x W 19 1/4" x D 31 5/8".

(2) (U) Mosler Model 30-39 Special Class 5 Single Door Security Cabinet. This cabinet is designed for closed-door operation. It contains fans and secured vents. Holes for power conduit mounting are not provided. The user may select the conduit mounting location (top, back, or side) and have mounting holes predrilled at the factory or may drill the holes after receiving the cabinet. The inside clear dimensions are H 25 3/4" x W 19 1/8 x D 34".

(3) (U) Mosler Model 30-31 Special Class 5 Single Door Security Cabinet. This cabinet is designed for closed-door operation. It contains fans and secured vents. Holes for power conduit mounting are not provided. The user may select the conduit mounting location (top, back, or side) and have mounting holes predrilled at the factory or may drill the holes after receiving the cabinet. The inside clear dimensions are H 25 3/4" x W 19 1/8" x D 25".

**e. (U) Security for Other COMSEC Material.** The following COMSEC Material will be safeguarded IAW AR 380-5:

(1) (U) General COMSEC instruction documents (KAG).

(2) (U) COMSEC equipment operating instructions (KAO).

(3) (U) COMSEC equipment maintenance manuals (KAM) other than cryptographic media.

(4) (U) Crypto-ancillary material (including hardware or software).

(5) (U) Other types of COMSEC material not specifically covered in this chapter.

**f. (U) Secured Storage Areas.** Each secure area or container used for the storage of classified COMSEC information will be kept locked when not under the direct supervision of authorized personnel.

**g. (U) Restrictions on the Use of Storage Containers.** There are many items that are the primary targets of thieves (e.g., money, precious metals, jewelry, weapons, narcotics, night vision devices). These items will not be stored in vaults, security containers, secure areas, or other areas used for the storage of classified COMSEC material. In an emergency, when adequate storage facilities are not available, the commander may authorize an exception to this restriction. This exception will be on a **temporary basis only** (see paragraph 5.10.4a.).

**h. (U) Lock Combinations.**

(1) (U) The combinations of locks used to secure classified COMSEC information in storage areas or containers will be safeguarded, changed, and recorded IAW AR 380-5.

(2) (U) A Standard Form (SF 700) "Security Container Information" will be maintained for each vault, secure room, container or drawer having a separate combination.

(3) (U) Lock combinations will be controlled and provided to a minimum number of authorized personnel.

**i. (U) Material Used to Process Classified COMSEC Information.** Typing ribbons, diskettes, and disks, which have been used to process classified COMSEC information, will be safeguarded as directed by AR 380-5.

## 5.11 TRANSPORTATION OF COMSEC MATERIAL.

**a. (U)** The possibility of compromise is increased during shipment. It is imperative that persons handling COMSEC material in COMSEC logistics (CMCS) channels and DoD standard logistics channels are carefully instructed in proper handling procedures, including emergency destruction procedures. Transportation in this context does not include moving a cryptosystem between operational sites by authorized movers.

**b. (U)** The following are the preferred methods of transporting key and other classified COMSEC material:

- (U) Defense Courier Service (DCS) (use DCS Form 1).
- (U) State Department Diplomatic Courier Service.
- (U) Officially designated couriers.

**c. (U)** Authorized means of transportation will ensure proper handling, equipment integrity during shipment, minimum stopovers and delays, on-time arrival, and reduced possibility of compromise.

**d. (U)** Instructions for marking and shipment of CCI material are contained in DA PAM 25-380-2.

## 5.12 KEYING MATERIAL MARKED "CRYPTO."

(U) The control procedures specified in the following paragraph apply to all key marked "CRYPTO," whether classified or unclassified.

**5.12.1 (U) Preparation for Shipment.**

**a. (U) Each COMSEC Custodian is responsible for:**

(1) (U) Making sure key is properly prepared for shipment.

(2) (U) Making sure only authorized shipping methods are used.

(3) (U) The accuracy and timeliness of all accounting and Transfer Reports.

**b. (U) Wrapping.** Prior to shipment, key will be double-wrapped and securely sealed using gummed paper-reinforced tape (NSN 8135-00-598-6097). Scotch or masking tape will not be used. Key will be packaged separately from its associated COMSEC equipment unless the application or design of the equipment is such that the key cannot be physically separated.

**c. (U) Marking Packages.** All packages will be clearly and adequately marked as follows:

(1) (U) Inner Wrappings. Conspicuously mark inner wrappings as follows:

(a) (U) Classification (if any).

(b) (U) The marking "CRYPTO."

(c) (U) All security markings, special handling instructions, and notations such as: THIS PACKAGE CONTAINS ACCOUNTABLE COMSEC MATERIAL - TO BE OPENED ONLY BY THE COMSEC CUSTODIAN.

(d) (U) TO and FROM address information: using geographic locations, not post office boxes.

(e) (U) COMSEC Account Numbers.

(f) (U) The instruction, ATTN: COMSEC Custodian, or equivalent.

(g) (U) The transfer documentation for the keying material shipment will be placed in a separate envelope. The envelope will be attached to the inner wrapper of the number one package of the shipment.

(2) (U) Outer Wrapper. The outer wrapper will contain only those markings necessary to facilitate delivery.

(a) (U) TO and FROM addresses: using geographic locations, not post office boxes. If package is being delivered via DCS, the outer wrapper will contain the two-line DCS address, COMSEC account number, ATTN: COMSEC Custodian, etc.

(b) (U) The outer wrapper will not display any markings that reveal package contents or that the package contents are classified.

(c) (U) Packages, which are to be shipped by courier, will be marked VIA COURIER or with other markings, as may apply. Material transmitted by State Department Diplomatic Pouch will indicate that COURIER ACCOMPANIMENT IS REQUIRED.

**5.12.2 (U) Methods of Shipment.**

**a.** (U) Preferred methods for shipping key is in the custody of formally authorized couriers identified in paragraph 5.11.b.

**b.** (U) Key classified SECRET will not be sent through the U.S. postal channels without prior approval from HQDA (DCS G-2). The use of commercial carriers to transport keying material is specifically prohibited.

**c.** (U) U.S. Registered Mail may be used to ship unclassified and individual editions of CONFIDENTIAL key (or extracts) to users in the U.S. and to activities served by U.S. postal facilities (to include APO/FPO facilities). Under no circumstances will the shipment pass through a foreign postal system or any foreign inspection.

**d. (U) Transportation of key via U.S. Flag aircraft within CONUS is authorized; however, outside of CONUS it is strongly discouraged due to the risk of terrorists and lack of U.S. control** (see AR 380-40, paragraph 2-17a).

## 5.13 COMSEC EQUIPMENT AND COMPONENTS.

(U) The following methods will be used for the shipment of classified COMSEC equipment and components. Other methods of transportation will not be used without prior approval from HQDA, (DAMI-CD).

**a.** (U) Defense Courier Service (DCS).

**b.** (U) U.S. Diplomatic Courier Service.

**c.** (U) Officially designated and cleared courier.

**d.** (U) Cleared commercial carrier, which provides Protective Security Service (PSS).

**5.13.1 (U) Use of U.S. Commercial Passenger Airlines.** Scheduled U.S. commercial passenger airlines may be used by cleared and designated U.S. military personnel and government civilian employees to transport classified COMSEC equipment and components at the discretion of the local commander,

provided the provisions of AR 380-5 are followed.

**a. (U)** The use of foreign carriers must be approved by HQDA (DAMI-CD).

**b. (U)** COMSEC equipment will not be shipped keyed unless its physical configuration/ engineering design makes it impossible to separate the key from the equipment. See paragraph 5.13.2 for exceptions.

**c. (U)** Items marked "CONTROLLED CRYPTOGRAPHIC ITEMS" (CCI), which are un-keyed, will be shipped IAW DA Pam 25-380-2. The following are basic principles that commanders must focus on when deploying in support of contingency operations and routine shipments to minimize the opportunity for loss/theft of CCI:

(1) (U) *Planning for unit shipments during contingency operations*. Commanders should have a detailed plan available that includes security during pre-deployment, deployment, employment, sustainment, and redeployment.

(2) (U) *Security of equipment in vehicles*. CCI should not be left unsecured in vehicles. These items should be secured in a rack, the vehicle locked in a motor pool or secured in locked unit containers with equipment of comparable value and sensitivity, and accounted for in accordance with established supply procedures.

(3) (U) *Rail shipments*. Units should coordinate with security and transportation personnel to determine the transportation security requirements for the type of equipment being shipped. CCI shipped via rail flatcar will be placed in locked MILVANs or CONEX containers and locked with high-security locking devices (see paragraph 5.9a). The door of the container must be inaccessible to preclude entry. To accomplish this, the container should be positioned on the flat car so the door is flush against an immovable object and door-to-door if more than one container is utilized. If needed, negotiate with the carrier through the military traffic management command to place an empty container on the rail car to preclude leaving a full container vulnerable. If, at any time, the security risk increases, use of supplemental security measures, such as unit guards, is encouraged.

(4) (U) *Inventorying*. Units must initiate inventories of equipment prior to shipment, which includes, as a minimum, serial numbers, nomenclature, and quantity. A copy of the inventory should be maintained in unit files and a copy placed in the vehicle or shipping container.

**5.13.2 (U) Protecting Classified COMSEC Equipment While in Transportation Channels.**

**a. (U)** The preferred method of protecting classified COMSEC equipment while in transportation channels is by one of the methods in subparagraphs 2-17b(1) and (2) of AR 380-40. In the interest of minimizing risk, commanders are directed to make every effort to satisfy their operational needs using the modes of transportation authorized, and through the use of couriers or escorts to protect sensitive COMSEC equipment. When such methods are not feasible, a request for waiver from HQDA (DCS G-2) is required.

**b. (U)** EXCEPTION: Within CONUS only, when operational necessity or contingency circumstances dictate, SECRET and CONFIDENTIAL classified COMSEC equipment installed in an enclosed vehicle or equipment shelter (e.g., MSE/ SINCGARS) may be transported via un-cleared commercial carriers, provided ALL of the following stipulations are strictly adhered to:

(1) (U) The determination of necessity to deviate from preferred transportation modes must be based on the commander's own risk assessment and his/her personal acceptance of that risk.

(2) (U) The classified COMSEC equipment and all systems within the vehicle or shelter must be completely zeroized and purged of all cryptographic key, crypto-ignition keys, etc., except as provided for in subparagraph 2-17b of AR 380-40.

(3) (U) The classified COMSEC equipment must be protected by tamper-detection/tamper-proof labels installed per instructions contained in National Security Agency (NSA)-published Protective Technology Implementation Procedures, applicable to the COMSEC equipment and/or specific type of tamper-proof label being utilized.

(4) (U) The classified COMSEC equipment must be secured in its shelter mounting by a steel locking bar that is locked in place with combination padlocks meeting Federal Specification FF-P-110, Sergeant & Greenleaf Model 8077A (NSN 5340-00-285-6523).

(5) (U) The vehicle or shelter containing the classified COMSEC equipment must be completely enclosed, and all openings covered from both the inside and outside to shield the interior from view. The entrance or door shall be secured with a high-security combination padlock as specified in the preceding paragraphs.

(6) (U) The vehicle or shelter should be banded across all openings with steel strapping, 1-1/4" wide, 0.035" wide, 0.035" thick (NSN 8135-00-283-0671) to further deter theft or attempted forced entry.

**c. (U)** The selected commercial carriers must certify that they utilize a system that accurately reflects a continuous chain of accountability for the material while it is in-transit, and:

(1) (U) Is a firm incorporated in the U.S.

(2) (U) Guarantee delivery within a reasonable number of days, based on the distance to be traveled.

(3) (U) Have a means of tracking the shipment in-transit and be able to pinpoint the location of the shipment upon request of the government representative.

(4) (U) Guarantee that the shipment will be afforded a reasonable degree of protection from theft or vandalism.

**5.13.3 (U) Packaging.** COMSEC equipment and components will be packaged and shipped as directed by AR 380-5: with the exception that COMSEC equipment packaged as follows are considered to be adequately packaged.

**a. (U)** Specially constructed fiberboard cases.

**b. (U)** Metal cases.

**c. (U)** Wooden boxes crisscrossed with metal (or equivalent banding strength) bands. When packaged in this manner, the inner opaque wrapper as called for by AR 380-5 may be omitted.

**5.13.4 (U) Contents Identification.** The contents of COMSEC equipment and component containers will be identified IAW MIL-STD 129D. CCI is marked IAW DA PAM 25-380-2.

**a. (U)** Outer Wrapper**.** The outer wrapper will not display any markings that reveal package contents or that the package contents are classified. The outer wrapper will contain only those markings necessary to facilitate delivery: TO and FROM addresses using geographic locations, not zip codes. If a package is being delivered via DCS, the outer wrapper will contain the two-line DCS address and COMSEC account number, ATTN: COMSEC Custodian. The outer wrapper may also be marked to indicate the number of packages in the shipment (e.g., 1 of 5, 2 of 5).

**b. (U)** Inner Wrapper. The inner wrapper will contain information identifying the contents. Transfer documentation for the equipment shipment will be placed in a separate envelope. The envelope will be attached to the inner wrapper of the number one package of the shipment.

**c. (U)** All COMSEC accounts, including Tobyhanna Army Depot (TYAD), will ship unclassified COMSEC material, EXCEPT key and CCI material, via First Class Mail. Other shipping methods, such as Registered Mail, may be used when dictated by transportation regulations, shipment size, cost or value or operational necessity. For CCI refer to DA Pamphlet 25-380-2.

## 5.14 CRYPTOLOGIC MEDIA.

**a. (U)** Cryptologic media is any media which embodies, describes, or implements a classified cryptologic. Cryptologic media will not be sent through any mail system. Cryptologic examples include:

(1) (U) Full maintenance manual (KAM).

(2) (U) Cryptologic descriptions.

(3) (U) Drawings of Cryptographic logic.

(4) (U) Specifications describing a cryptographic logic.

(5) (U) Cryptographic computer software.

**b. (U)** Cryptologic media will be transported by a properly cleared:

(1) (U) Department courier.

(2) (U) Service courier.

(3) (U) Agency or contractor courier.

(4) (U) DCS courier.

(5) (U) U.S. Diplomatic Courier Service.

## 5.15 SHIPMENT OF CLASSIFIED WITH UNCLASSIFIED COMSEC MATERIAL.

(U) Unclassified and classified COMSEC material may be shipped together only when there is an urgent operational need to provide both types of material simultaneously.

## 5.16 COURIERS.

**5.16.1 (U) Courier Requirements.** Official couriers of classified COMSEC material will be so designated, in writing, by the commander or his/her authorized representative. COMSEC material being hand carried from one geographical point to another (e.g., between installations/government facilities) including keyed or un-keyed CCI, must be couriered by an authorized individuals appointed on courier orders. AR 380-40 and AR 380-5 refer to the use of a Courier Authorization Card (DD Form 2501). This card serves only as a means to identify the individual as an authorized Government Courier. AR 380-40 also refers readers to AR 380-5, Chapter 8, for additional guidance, which states that a courier must be provided a written statement in addition to the DD Form 2501. This official document (Courier Orders) identifies the individual as a courier; the material the courier is authorized to hand carry; briefing instructions regarding who is to receive the material and how the material is to be transported, handled, and controlled; how the material is to be stored in transit (overnight stopovers, etc.); and, what to do in case of emergency, loss, or compromise of material.

The following requirements apply to all couriers:

**a. (U) Security Clearance**. Couriers will be properly cleared for the level of classified material they are transporting.

**b. (U) Safeguarding the Material**. The designating authority will make sure couriers are briefed on how to safeguard material that is in transit. Safeguarding the material is particularly important during delays and stopovers.

**c. (U) Weapons Requirement**. The commander will determine the need for carrying weapons. Couriers will not normally be armed; however, if the tactical or environmental conditions warrant the use of weapons, they will be issued and couriers will be briefed on their use, as appropriate.

**5.16.2 (U) Courier Responsibilities.**

**a. (U) Material Safeguarding**. Couriers are responsible for ensuring the integrity of the COMSEC material in their custody at all times.

**b. (U) Transporting into Foreign Countries.** See paragraph 5.12.2d for transportation requirements.

**c. (U) Last-On-First-Off Procedure**. When the physical bulk or configuration of the material being transported will not permit the courier to keep the material on his/her person or in view at all times, prior arrangements will be made with the carrier to effect a “last-on-first-off” procedure (courier will ensure the material is the

last item loaded and the first item unloaded). This procedure ensures the material will not be moved without the courier being present.

**d. (U) CRYPTO Key Escort**. The courier will escort CRYPTO key at all times. Should the material be placed in a locked compartment during shipment, the courier will check the locked area as frequently as possible.

**5.16.3 (U) Airdrop of COMSEC Material.** COMSEC material may be air-transported and airdropped to its destination when necessary due to tactical operating conditions. Air transportation and airdrop of certain COMSEC material may be prohibited by specific cryptosystem regulations or handling instructions. Units must check appropriate regulations and instructions prior to shipment by these methods. The following criteria will be observed:

**a. (U) Security Control**. Airdropped COMSEC material will be under the control of a properly cleared individual prior to and during flight, and until such time the material leaves the aircraft.

**b. (U) Material Recovery.** Authorized personnel will not airdrop COMSEC material unless there is a high probability of immediate recovery.

**c. (U) Sling-Loaded COMSEC Equipment.** When required in support of forward tactical operations, vehicles or shelters, which contain un-keyed COMSEC equipment, may be transported using sling-loading methods. Sling-loaded COMSEC equipment will not be keyed unless the equipment is required for immediate operation upon landing. COMSEC key will not be sling-loaded but may be transported inside the helicopter.

## 5.17 EMERGENCY PLANS AND PROCEDURES.

(U) This paragraph contains procedures for preparing, practicing, and executing emergency plans as directed by AR 380-40. The commander will make sure the following items are considered when preparing and executing emergency plans.

**a. (U) Planning for Hostile or Emergency Actions.** This planning must concentrate on actions to safely evacuate or securely destroy COMSEC material. Plans must be realistic, simple and workable. As the following reflects, CONUS and OCONUS requirements differ:

(1) CONUS: Emergency plans for CONUS are strongly recommended, but not required. However, for COMSEC accounts that are deployable, the custodian must ensure that an emergency plan is developed once the account is deployed OCONUS. See AR 380-40, Chapter 3.

(2) OCONUS: All Army activities outside the U.S., its territories, and its possessions (to include Alaska, Hawaii, Puerto Rico, Guam and the Virgin Islands), which hold COMSEC material, must maintain a current, written emergency plan for the protection of such material during emergencies.

**b. (U) Training Exercises.** Exercises to train personnel in the execution of Emergency Plans will be conducted as prescribed in Chapter 3, AR 380-40. They should simulate the real situation, include as many concerned personnel as possible, and stop just short of actual emergency execution. The following training information will be recorded as a Memorandum For Record (MFR) and filed with the emergency plan:

(1) (U) The latest date of training.

(2) (U) Types of plans tested.

(3) (U) Training results.

(4) (U) Names of participating personnel.

**c. (U) Precautionary Destruction and Evacuation.** During actual emergency conditions, precautionary destruction or evacuation of COMSEC material should not be delayed because of uncertainty as to threat/risk conditions, or for monetary considerations. Destruction priorities are specified in paragraph 5.20.4. COMSEC material replacement after a crisis is significantly less costly than a damage assessment to national security after a compromise.

## 5.18 PREPARATION OF EMERGENCY PLANS.

**5.18.1 (U) Provisions.** The following provisions, as appropriate, may be incorporated into emergency plans.

**a. (U)** Authorization for the senior member present to implement the plan.

**b. (U)** Assignment of specific responsibilities by duty position, rather than by name, with designated alternates.

**c. (U)** Location of combinations to containers of COMSEC material.

**d. (U)** Location of COMSEC material by storage container.

**e. (U)** Removal of accounting records (e.g., IR Cards, automation back-up disk, and H/R files) to facilitate the post emergency inventory.

**f. (U)** Designation of the evacuation site or alternate site. Include the routes and alternate routes of travel.

**g. (U)** Procedures for removal or destruction of hard drives, other AKMS automation components, and software containing key management and other classified or sensitive data base information.

**h. (U)** Location of fire-fighting equipment.

**i. (U)** Instructions for admitting firemen and other un-cleared emergency personnel to the COMSEC Facility, and provisions for safeguarding the COMSEC material during such access.

**j. (U)** Provisions for packing, loading, and transporting COMSEC material and for its safeguard during transit. In addition, consideration should be given to the evacuation of emergency destruction material that will be used during transit or at a later date.

**k. (U)** Provisions for the removal of key, if applicable, from equipment, and the storage thereof when emergency storage is to be implemented.

**l. (U)** Location of destruction implements.

**m. (U)** Provisions for precautionary disposal action.

**n. (U)** Annual review of the plan and assigned duties by all personnel.

**o. (U)** Procedures for unannounced, simulated, emergency training exercises.

**p. (U)** Reporting instructions before, during and after execution of emergency plans, during training or actual emergencies. Include “lessons learned” in after-action reports.

**q. (U)** Emergency plans, which contain classified information, must be securely stored as specified in AR 380-5.

**5.18.2 (U) Coordination.** Emergency plans involving COMSEC material will be coordinated with or incorporated into higher command emergency plans. This will ensure that evacuation, storage, and/or destruction will be effectively and securely performed as part of the overall command OPLAN in the event of an actual emergency.

## 5.19 RECOMMENDED EMERGENCY TASK CARDS.

**a.** (U) Task cards are used for preparing emergency plans. Within certain COMSEC Facilities, task cards may not be appropriate or feasible. In this case, the decision to use task cards rests with the commander.

**b. (U)** In case of an emergency, the senior person present must implement the emergency plan.

**5.19.1 (U) Task Cards.**

**a. (U)** First, identify each specific task and assign a priority for accomplishment. Then, record the task and the approximate time for completion (write clearly and concisely) on its own 5x8 card.

**b. (U)** In an emergency, personnel will report to a pre-designated location. The person in charge or another designated individual will issue the task cards to individuals one at a time, based on priority. Each individual will then carry

out the designated task as written on the card and return to the person in charge to report that the task has been completed. This individual will then be given another task to be completed. This procedure will continue until all tasks have been completed. Under this system, many tasks are being completed at the same time, maximum personnel usage is employed, and the progress of emergency actions are known at all times.

**5.19.2 (U) Sample Task Cards.** The sample task cards addressed in the following paragraphs do not necessarily include all actions required at a facility. Additions, changes and modifications to the instructions on these sample cards will be necessary to accommodate the specific conditions and circumstances at a particular facility. For example: It may not be practical to put the safe combinations (which must be stored securely) on task cards and at the same time conveniently store the cards to permit easy access. Sample task card instructions are as follows:

**a. (U) TASK CARD 1.**

(1) (U) Go to room XX and remove the IR Card file from the storage cabinet just inside the door. Take the file to room XX. Go to the incinerator in room XX. Get it fired up.

(2) (U) Place the material received into the incinerator in the order in which it was received. Using the IR Card file, check off the items as they are destroyed. Tend the incinerator until all material has been burned. Report back to the person in charge.

**b. (U) TASK CARD 2.** Two individuals will go to the storage cabinet just inside the door to room XX. With the key attached to this card, unlock the cabinet, remove the three M-3 Sodium Nitrate Destruction Kits. Load them on the dolly located next to the cabinet, and roll them down the corridor and out the exit. Set up the kits in the courtyard as you have been instructed. As soon as the kits are set up and ready to accept material, one of you report back here to me. The other one remain with the kits and load material into the kits; wait for further instructions from the person in charge or someone acting on his/her behalf.

## 5.20 EMERGENCY MEASURES.

(U) Measures, which can be taken in the event of an emergency, include EVACUATION, SECURE STORAGE, and DESTRUCTION. The commander will decide which of these measures will be taken and will indicate in the plan those measures not considered feasible. Evacuation and/or secure storage will be considered before destruction. However, simultaneous implementation of any two or all three measures may be necessary.

**5.20.1 (U) Emergency Evacuation.**

**a.** (U) Evacuation is defined as the removal of COMSEC material to a SAFE, alternate location. The removal of COMSEC equipment must be performed in a systematic manner and under the direction of a responsible individual.

**b.** (U) When evacuating COMSEC material, every effort will be made to prevent loss or unauthorized access; special care must be exercised during the period from the evacuation to the subsequent return of the material to its original location or the relocation to a new secure area.

**c.** (U) There are several factors that influence the decision to evacuate COMSEC material:

(1) (U) Time available.

(2) (U) Future requirements for the COMSEC material.

(3) (U) Degree of hazard involved in the removal.

(4) (U) Safety of the new location.

(5) (U) Means of transportation available.

(6) (U) Transportation routes available.

**5.20.2 (U) Secure Storage During an Emergency.**

**a. (U)** Secure storage in an area at risk is not an effective emergency measure while under the threat of enemy attack.

**b. (U)** Secure storage during other types of emergencies can be achieved by using authorized vaults, safes, or a secure room. If a secure room is used, all classified boards must be removed from non-secured COMSEC equipment and stored along with classified components and other classified COMSEC material in approved security containers.

**c. (U)** If possible, a guard should remain in or near the storage area. The placement of guards in the area as a secondary barrier is desirable. However, a guard does not satisfy basic emergency storage requirements.

**d. (U)** Various factors, which would influence the decision to secure COMSEC material in place, are as follows:

(1) (U) Time available.

(2) (U) Nature of the emergency (whether by human or natural causes).

(3) (U) Seriousness of the emergency.

(4) (U) Possibility of returning to the site.

(5) (U) Bulk and weight of the material (in deciding whether to store or evacuate).

**5.20.3 (U) Emergency Destruction.** Destruction of key includes zeroizing COMSEC equipment and removing and destroying the current key card or key list extract. Plans for COMSEC Facilities holding classified operational key will include provisions for the emergency destruction of such key.

**5.20.4 (U) Priorities. USED, SUPERSEDED,** classified key marked "CRYPTO" is the **MOST SENSITIVE** of all COMSEC material. It must be given the **HIGHEST DESTRUCTION PRIORITY** to prevent its compromise. The general priority for emergency destruction of COMSEC material is as follows:

***(U) Priority 1.*** All superseded and current classified key marked "CRYPTO" in that order except authenticators, CONFIDENTIAL tactical operations codes, unused OTP and OTT, and unused point-to-point (two copy) key.

***(U) Priority 2.*** TOP SECRET multi-holder key that is to become effective within the next 30 days.

***(U) Priority 3.*** Superseded tactical operational codes.

***(U) Priority 4.*** SECRET and CONFIDENTIAL multi-holder key, which is to become effective within the next 30 days.

***(U) Priority 5.*** Sensitive pages of crypto-equipment maintenance manuals (or the complete manual).

***(U) Priority 6.*** Classified components or sub-assemblies of COMSEC equipment (printed circuit boards and module boards) in the order listed in the appropriate maintenance manuals.

***(U) Priority 7.*** The balance of the COMSEC equipment maintenance manuals and classified operating instructions.

***(U) Priority 8.*** All remaining classified COMSEC material and unclassified key marked "CRYPTO." Superseded authenticators and unused two-copy key will be destroyed, if time permits.

## 5.21 EMERGENCY DESTRUCTION METHODS AND MATERIALS.

**(U) Destruction Methods and Materials.** It is the responsibility of the commander to select appropriate emergency destruction measures for a COMSEC Facility. This selection should be based on a comprehensive risk assessment and threat evaluation, conditions at each facility and the available destruction alternatives. Destruction procedures and methods are as follows:

**5.21.1 (U) Key and COMSEC Documents.** When there is an emergency situation, key and other classified COMSEC publications will be destroyed based on priority, as specified by the commander in the Emergency Plan. If this is not possible, any method may be used which, in the judgment of the senior person present, will result in the least likelihood of unauthorized access or recovery. Any devices or method approved for routine destruction is acceptable.

**5.21.2 (U) Shredders.** Any type of shredder may be used when other methods of destruction are not available and the key is mixed with an

equal amount of other material of similar composition. Shredders may also be used as a supplementary method to speed destruction, when necessary. Shredded key, when sized larger than 1.2 mm (0.05 inches) in width and 13 mm (0.5 inches) in length, or as an alternative, 0.73 mm (0.03 inches) in width and 22.2 mm (0.87 inches) in length, will be scattered or dispersed over a wide area.

*WARNING*

SODIUM NITRATE

**5.21.3 (U) Sodium Nitrate Destructors.** Magnetic tape on aluminum reels or metal components of COMSEC equipment (especially aluminum or magnesium) will **never** be placed in Sodium Nitrate Destructors since a severe explosion hazard exists. Also, intense heat and a column of flames as high as 20 feet are generated whenever the M3 or M4 Document Destroyer is used. Personnel will remain at a safe distance for 20 minutes after ignition. The M3 and M4 will only be used out-of-doors in an area free from overhead obstructions or other objects that may catch fire. The molten slag reacts violently when coming into contact with cold or wet surfaces.

**a. (U) Document Destroyer Kit M4 (NSN 1375-00-078-0450-M 814).** Document destroyer kit M4, or other prepared kits, may be used for document destruction (refer to TB-CML-110).

(1) (U) The M4 device consists of:

(a) (U) A 55-gallon metal outer drum.

(b) (U) A fiberboard inner drum.

(c) (U) 190 pounds of prilled sodium nitrate loaded in the space between the outer and inner drums.

(d) (U) 3 tubular bags of ignite mix.

(e) (U) 2 each M-72 railroad fuses.

(f) (U) Other items, including screen cover, outer drum cover, inner drum cover, lever lock ring, gasket, plastic foam spacers, and miscellaneous packing material.

(2) (U) This device is capable of destroying a maximum of 12 pounds of paper or mixture of paper, plastics, film, magnetic tape on nonmetallic reels, and printed circuit boards. The composition of items to be destroyed should be within the following limits:

(a) (U) Cellulose paper (documents) 70-100 percent.

(b) (U) Plastics (printed circuit boards), 20 percent maximum.

(c) (U) Film or magnetic tapes on non-metallic reels, three percent maximum.

(d) (U) Paper must be intermixed with plastics, film and tapes to effect complete destruction.

**b. (U) Document Destroyer, Emergency, Incendiary, M3 (NSN 1375-00-529-8004-M605).**

(1) (U) The M3 kit consists of:

(a) (U) 5 each 19 lb packages of sodium nitrate.

(b) (U) Igniter charge.

(c) (U) Screen.

(d) (U) Retaining ring assembly.

(e) (U) Two igniters.

(f) (U) Box of safety matches.

(2) (U) The device is capable of destroying a maximum of 100 pounds of paper or mixture of materials of the same composition and ratios as stated in the preceding paragraph for the M4 Document Destroyer. To use the M3 kit you must obtain a clean 55-gallon drum, open at one end. A metal cover with a 6-inch-to-8-inch diameter hole must be

provided for the 55-gallon drum in order to maintain sufficient pressure inside the drum to ensure complete combustion. The M3 is employed as follows:

(a) (U) Open the kit. Remove one package of sodium nitrate and spread its contents over the bottom of the drum: breaking up any lumps.

(b) (U) Scatter about one fourth of the material to be burned over this layer of sodium nitrate and follow with another layer of sodium nitrate. Paper and books need not be torn up. Printed circuit boards to be destroyed must be mixed with paper; otherwise, destruction will not be accomplished.

(c) (U) Continue to alternate layers of sodium nitrate and paper: spreading and breaking the lumps in each package of sodium nitrate until the last fourth of material to be burned has been added.

(d) (U) Add the last package of sodium nitrate and the ignition charge. Mix this layer with paper. Do not scatter the ignition charge.

(e) (U) Place the metal band around the drum directly below the top-rolling hoop. Fasten the band by passing the end through the ring on the other end and bending it back.

(f) (U) Cover the drum with the metal screen and attach the wires on each corner of the screen to the corresponding "D" rings on the metal band. Do not punch holes in the drum.

(g) (U) Remove the tape holding the lever to the body of the igniter. Hold the lever tightly to the body of the igniter and remove the safety pin.

(h) (U) Insert the fuse end to the igniter through the hole in the metal screen and drop the igniter into the incinerator drum. The igniter has a 1.2 to 2 second delay before ignition (see TM 43-0001-38, page 6-8).

(i) (U) An additional igniter and box of matches are provided should the first attempt fail.

*WARNING*

SODIUM NITRATE

**Magnetic tape on aluminum reels or equipment components made of larger amounts of metal (especially aluminum or magnesium) must never be destroyed in the container utilizing the ABC-M4 since a severe explosion hazard exists. Use of the ABC-M4 generates intense heat and large amounts of flame and toxic smoke. Areas in which the ABC-M4 is activated will be IMMEDIATELY EVACUATED.**

**c. (U) File Destroyer, Incendiary, ABC-M4 (NSN 1375-00-219-8564-M610).**

(1) (U) Installation of the ABC-M4 in a filing cabinet or security container takes up approximately 60 percent of the usable drawer space. For this reason, planning must take into account the destruction of any classified material that must be removed from the file drawers (refer to TB-CML-110). The ABC-M4 consists of:

(a) (U) A wooden crate containing 44 oxidizer panels filled with sodium nitrate.

(b) (U) 4 igniter panels with wiring harnesses.

(c) (U) 4 chain-link metal mats.

(2) (U) Two ABC-M4 kits are required to destroy the contents of a standard 4-drawer security container. The oxidizer panels are interlaced at 1 or 2-inch intervals through the file drawers with 1 or 2 igniter panels placed in each

drawer. The chain-link mats are placed on top of the paper in each drawer to keep it compressed during destruction. Destruction is accomplished with drawers in the closed position. Activation is normally accomplished electrically by attaching the igniter panel wiring harnesses to a truck battery or other voltage source. Each igniter box contains two squibs connected in parallel to a pair or igniter wires that are used to connect the squibs to a power source.

(a) (U) One oxidizer panel is installed in the front of each file drawer and one behind each 1/2-inch thickness of paper in the drawer until all papers in the drawer are sandwiched between oxidizer boxes.

(b) (U) An igniter panel is placed ahead of the first oxidizer box in each file drawer.

(c) (U) The squib wires from each drawer must be extended out of the drawers with care in a manner to prevent them from being cut or broken when the drawers are closed. The wires are brought together so they may be easily connected to the firing line.

(d) (U) A chain-link mat is placed on top of the papers and panels in each drawer so that it will remain in contact with the contents of the file as burning progresses.

(e) (U) The drawers are closed.

(f) (U) The squib wires are connected in parallel to a firing lead.

(g) (U) A blasting machine or other source of electricity is used to fire the squibs, which sets fire to the wood-flour-and sodium nitrate mixture. The sodium nitrate furnishes oxygen to support combustion in the closed file. Papers adjacent to the igniter panel ignite and the sodium nitrate in the next oxidizer panel furnishes the necessary oxygen for combustion. Combustion progresses in this way until the entire contents of the drawer are burning. The weight of the rack keeps the contents of the file compressed, thereby providing maximum contact between the paper and the sodium nitrate and maximum effectiveness of the incendiary. A file destroyed by an ABC-M4 incendiary emits large volumes of acrid black smoke while burning; therefore, the area should be evacuated until burning is complete and the area is ventilated.

(h) (U) If possible, following an active burn period (approximately 20 minutes) and a sufficient cool-down time, containers in which ABC-M4's have been activated will be re-opened and the contents inspected. These devices, especially older ones, are not completely reliable and some unburned or partially burned material may still remain.

(3) (U) Fuels, kerosene, gasoline, and sodium nitrate may be used to expedite burning. Extreme care must be used for personal safety.

*WARNING*

SODIUM NITRATE

(U) Magnetic tape on aluminum reels or metal components of COMSEC equipment (especially aluminum or magnesium) will **never** be placed in Sodium Nitrate Destructors since a severe explosion hazard exists. Also, intense heat and a column of flames as high as 20 feet are generated whenever the drum is used. Personnel will remain at a safe distance for 20 minutes after ignition. The drum will be used only out-of-doors in an area free from overhead obstruction or other objects, which may catch fire. The drum must not be tipped over while contents are still actively burning. The molten slag reacts violently when coming into contact with cold or wet surfaces.

**d. (U) Sodium Nitrate Destructor Drums.** If prepared kits are not available, 120 pounds of sodium nitrate (spray-coated and pelletized, if available), two or three pounds of sugar, and a 55-gallon steel drum (20 gauge or heavier) can be used to destroy approximately 100 pounds of paper and from 15 to 20 printed circuit boards at the same time. The following directions apply:

(1) (U) Dump about 20 pounds of sodium nitrate into the bottom of the drum followed by 6 to 10 inches of paper and one printed circuit board. The paper should be flat.

(2) (U) Repeat with about 2 inches of sodium nitrate, 2 or 3 inches of paper and one printed circuit board until the drum is full, ending with a layer of sodium nitrate on top.

(3) (U) Make a starter charge by thoroughly mixing 2 or 3 pounds of sugar with an equal amount of sodium nitrate. Spread the mixture over the top layer.

(4) (U) Cover the drum. At lower altitudes, a 24-inch square of 5/8-inch wire mesh screen, weighted or wired to the drum, makes an adequate cover. At 3,000 feet or more above sea level, a lid with less ventilation than the screen must be devised. Such a lid may be improvised by cutting one or more holes in a regular steel drum lid. Hold the lid on with a wired-down screen mesh cover.

(5) (U) A combustible mixture such as rubbing alcohol can be sprinkled on the starter charge. Normally, this is not required as the fire can be started by means of a torch or burning paper applied to the starter charge. After the fire is started, the operator should retreat 50 feet or more. It may take up to 5 minutes for the fire to reach its full intensity.

**5.21.4 (U) Destruction of COMSEC Equipment.** COMSEC equipment will only be destroyed as a last resort to prevent it from falling into unauthorized hands. Destruction may be by any method that will render the equipment **unusable** and **irreparable.**

(U) Destruction will be accomplished to a degree that reconstruction of the cryptographic logic is not possible. Removing and destroying the classified assemblies and CCI components within the equipment, including classified printed circuit boards and multi-layer boards can do this. If the classified assemblies and CCI are destroyed, it is not necessary to totally destroy the remainder of the equipment. The following are approved and effective methods for the emergency destruction of crypto-equipment.

*WARNING*

SODIUM NITRATE

(U) Do not stare directly at the fireball caused by the ignition of the M1A2 or similar device: The intense light can cause eye damage. Extreme heat, intense flames and toxic smoke are caused by the ignition of these incendiaries. Personnel should remain at a safe distance for 15 to 20 minutes after ignition.

**a. (U) Thermite Incendiaries.** Thermite incendiaries will provide effective and total destruction **(not authorized for use in the U.S. except for training purposes)**. Ensure you have read the instructions to determine what is a safe distance away from the explosion.

(1) **(U) Cryptographic Equipment Destroyer, Incendiary, M1A2-TH4 (NSN 1375-00-834-8884-M598).** The M1A2 is a thermite incendiary measuring 10-1/2" x 15" x 1-1/2" and weighing 35 pounds. This device may be placed on the equipment exterior or on components, which have been removed (refer to TB-CML-110). The M1A1-TH1 and M2A1 are obsolete devices similar to the M1A2 and may still be found at some sites. The M1A1 is the same size and weight as the M1A2 although it is slightly less powerful and is charged with thermite rather than TH4 thermite. The M2A1 is a half-sized (16" x 8-1/2" x 1", 12 pounds) version of the M1A1. The number of M1A2 devices required for destruction varies

with the size and density of the target. The degree of destruction may be enhanced by placing target equipment or material in a close fitting pit in the ground or in a wooden or double-lined steel box. This prevents the molten slag, which accomplishes the actual destruction, from running off. The M1A2s should be placed one on top of the other and banded or taped to the equipment or material to be destroyed. Ignition of the M1A2 may be accomplished as follows:

(a) (U) Manually. Remove the tape holding the safety pin in place and remove the safety pin. There are three seconds before detonation.

(b) (U) Electrically. Make two leads by twisting together all wires of the same color and touching them to a voltage source. There are three seconds before detonation.

(c) (U) With the AN-M14 incendiary grenade. Pull the safety pin and place the grenade quickly on the top incendiary towards the front and between the detonators.

*WARNING*

SODIUM NITRATE

(U) This technique generates an intensely violent reaction with intense heat and light and large amounts of flame and toxic smoke. Personnel should remain at a safe distance for 15-20 minutes following ignition.

**b. (U) Field Expedient Equipment Destruction.** The following technique has been developed to totally destroy COMSEC equipment, after it has been **zeroized,** by using a combination of one M1A2 panel and 30-35 pounds of loose, prilled sodium nitrate.

(1) (U) Remove and discard equipment top, or open the drawer on rack-mounted equipment.

(2) (U) Remove and discard UNCLASSIFIED printed circuit boards.

(3) (U) Evenly relocate classified boards, if necessary.

(4) (U) Fill equipment chassis with loose, prilled sodium nitrate.

(5) (U) Place the M1A2 panel on top of equipment or drawer and ignite normally.

**c. (U) Grenade, Hand Incendiary, AN-M14 (NSN 1330-00-219-8557-G900).** Due to its small size and limited duration of burn, the AN-M14 grenade is only of marginal value in an emergency destruction. It may be used to ignite other devices such as the M4 or M3 drums or the M1A2 panel. The M14 may also be used, as a last resort, to destroy beyond reuse a small piece of equipment, single drawers of large rack-mounted equipment, or several stacked reels of magnetic tape.

**d. (U) Emergency Destruction Cable.** The following is a suggested procedure for simultaneously igniting several incendiaries by means of an "emergency destruction cable." The procedure is appropriate in overseas communications/signal centers where emergency plans call for the in-place destruction of several pieces of installed equipment. To prevent accidental ignition, one person will be designated to HOLD the AC plug until ignition is desired. The procedure is as follows:

WARNING

(U) In no case will the plug be connected to a power source that would place the incendiaries between the individual and the exit.

(1) (U) Fabricate a cable long enough to reach from a power source outside or near the door of the facility to each equipment position.

(2) (U) At the point where the cable passes each position, a pair of six-foot leadoff wires should be installed on the cable.

(3) (U) Install a male AC plug at the end of the main cable. In an emergency, the cable should be laid on the floor

throughout the facility so that it is within one foot from the base of each equipment position.

(4) (U) Place incendiaries on equipment and attach the incendiary leadoff wires to the six-foot pairs of the leadoff wires coming from the cable.

(5) (U) Double-check all connections and EVACUATE the facility.

(6) (U) Apply the AC male plug to a power source.

(7) (U) The existing emergency power light fixtures required in communications/ signal centers may be modified and used as an electrical source point to simultaneously ignite all incendiaries by throwing a single switch. A primary ignition voltage of 110/220 VAC, or a secondary ignition voltage of 6/12 VDC, would be applied to the cable via a common terminal point. The use of a switch to select the desired voltage would eliminate the necessity of physically changing wire connections or searching for an alternate battery source should the local power fail prior to ignition. The switch is wired in such a way that in one position the terminals are directly in parallel to the source voltage of 110/220 VAC and, in the other position, the voltage selected is in the battery voltage of 6/12 VDC should the power be off. In the center or "off" position, the terminals would be "open" or have no voltage applied at all. When the switch is off, the emergency destruction cable can safely be connected without fear of premature ignition of the incendiaries. The device also provides emergency lighting to facilitate the connection of the emergency cable if normal lighting is lost. The materials required (local purchase) are two binding post terminals and one toggle switch. The switch must be a three-position, DPDT, single-hold mounting which opens both sides of the circuit.

**g. (U) Fire Axes.** Printed circuit boards may be destroyed by hacking with an ax and scattering the pieces.

**5.21.5 (U) Destruction in Aircraft.**

**a. (U) Evacuation Over Water.** If an aircraft is operating over water and its capture or other emergency appears imminent, zeroize the COMSEC equipment and destroy key and associated material as completely as possible if time permits.

**b. (U) Evacuation Over Land.** If the aircraft is in danger of going down over land in a friendly zone, COMSEC equipment will be zeroized and all classified COMSEC material will be allowed to remain in the aircraft. However, if the aircraft is being forced down over a hostile area, first zeroize the COMSEC equipment. Every effort should be made to totally smash classified and CCI components beyond reuse. Shred or rip paper material to pieces and then jettison the residue and smashed components over the widest possible area.

## 5.22 DESTRUCTION OF COMSEC MAINTENANCE MANUALS.

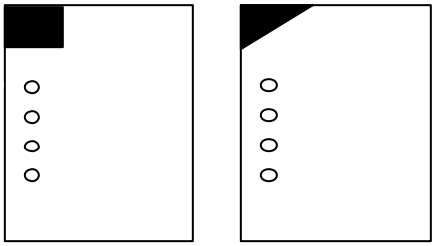
**a. (U) Sensitive Pages.** Destruction procedures will be as directed in paragraph 5.18.5a and shall apply to all organizations operating outside the U.S., its territories, and its possessions, with the exception of CLSFs holding KAMs for storage only. Each KAM contains, at the rear of the textual portions, either a list of sensitive pages or a statement that there are no sensitive pages in the KAM. In addition, some KAMs further identify their sensitive pages by means of gray or black diagonal or rectangular markings at the upper portion of the binding edge. During an emergency, there may be insufficient time to completely destroy the KAMs. Information contained in certain KAMs may consist largely of unclassified information with only a few extremely sensitive pages. The sensitive pages will be destroyed first, before the remainder of the KAM.

**b. (U) Preparing Sensitive Pages for Emergency Destruction.**

(1) (U) Apply distinctive markings (e.g., red stripes) to the binder edge and covers of all KAMs containing identified sensitive pages.

(2) (U) Remove each sensitive page from the KAM.

(3) (U) Cut off the upper left-hand corner of each sensitive page such that the uppermost binder hole is removed. Either of the cutting methods indicated is satisfactory.



(4) (U) When cutting off the page corner, use extreme care not to remove any text or diagrams from the page.

(5) (U) Reinsert all pages in their proper order and replace the screw posts, binder rings or multi-ring binder.

(6) (U) Conduct a page check.

**c. (U) Removing Sensitive Pages in an Emergency.**

(1) (U) Remove the screw post or binder rings, or open the multi-ring binder, and remove all pages from the KAM.

(2) (U) Insert a thin metal rod (wire, screwdriver, etc.) through the top hole of the KAM so that it extends completely through the manual.

(3) (U) Holding both ends of the rod, shake the entire manual vigorously. The sensitive pages should fall freely to the floor.

**d. (U) Test Exercise.** A text exercise should be conducted on each KAM to ensure that all sensitive pages will be removed by the procedure described in the preceding paragraph. After conducting such a test, care must be taken to ensure each page is correctly inserted into the manual. A page check should then be performed. Refer to paragraph 5.19 for emergency task cards.

## 5.23 ACTIONS AFTER AN EMERGENCY.

**a. (U) Report Requirements.** Whenever emergency plans are executed, message reports will be sent to CSLA with an information copy to the CONAUTH. In addition, an information copy will be sent to the CLSF, which provides COMSEC support, and to the unit's next higher headquarters. If the emergency action involves a COMSEC Incident, reports will be submitted as directed in Chapter 7 of this TB. Reports of emergencies are exempt from reports control under the provisions of AR 335-15.

**b. (U) Report Contents.** When reporting emergency conditions that do not result in a COMSEC Incident, as a minimum, units will perform the following:

(1) (U) List the material destroyed or relocated.

(2) (U) Indicate the method and degree of destruction.

(3) (U) Indicate the circumstances that caused the emergency plans to be executed.

(4) (U) Summarize resupply actions initiated or planned, if applicable.

**c. (U) Recovery of COMSEC Material.** When the execution of emergency plans results in the abandonment of classified COMSEC material, every reasonable effort will be made to recover the material at the earliest possible moment. Recovered classified COMSEC material or residue thereof, will be collected and placed under the control of appropriately cleared individuals until disposition instructions are received.

## 5.24 PRECAUTIONARY ACTIONS.

**a. (U)** When a situation develops that indicates an emergency plan may have to be executed, as a precaution, commanders must be prepared to immediately reduce COMSEC material holdings to the minimum necessary for continued operation. This precautionary action, prior to an actual emergency, will remove nonessential material from danger and simplify evacuation or destruction should they become necessary.

**b. (U)** The same priority listed in paragraph 5.20.3 for emergency destruction will apply for precautionary destruction except that, of necessity, current key must be retained in order to maintain secure communications.

**c. (U)** Future and contingency key and backup cryptosystems should be removed or stored, and all superseded material destroyed. At the first hint of an emergency, superseded key will be destroyed. Removal or storage of future key should be considered in preference to destruction. The commander, with advice from the COMSEC Custodian, will determine what material will be retained to continue secure communications and when to store, remove, or destroy material not required.

**d. (U) When material is destroyed as a precautionary measure, the appropriate issuing activity will be notified for the purpose of accounting and post emergency resupply.**



FOR OFFICIAL USE ONLY

**THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY**



FOR OFFICIAL USE ONLY

# CHAPTER 6

# ARMY KEY MANAGEMENT SYSTEM (AKMS)

## 6.1 GENERAL.

(U) The AKMS provides local real-time electronic key generation, distribution, and management in support of C4I at all levels. It provides accountability and management of existing COMSEC material now being maintained by Army COMSEC accounts worldwide. The AKMS ensures compatibility and interoperability between all services within DoD and replaces the current Army automated COMSEC software (ACCLAIMS), as well as the majority of manual COMSEC accounts. AKMS also provides for electronic distribution of Modern key, such as that key used for keying STU-III, Secure Telephone Equipment (STE), Secure Data Network System (SDNS), and other FIREFLY-based COMSEC encryption equipment.

**6.1.1 (U) Primary Tier 1 Sites (PT1S).** For the purpose of this TB, all references to COR pertain to the Primary Tier 1 Sites (PT1S) to which the AKMS COMSEC accounts are serviced (i.e. Lackland AFB, Texas or Fort Huachuca, Arizona). A Service Authority has been assigned for each service. Only those actions that are specific to an AKMS COMSEC account will be addressed in this chapter. All other actions required for the maintenance and accountability of Army COMSEC accounts are addressed elsewhere in this TB.

## 6.2 LOCAL COMSEC MANAGEMENT SOFTWARE (LCMS) WORKSTATION.

**6.2.1 (U) Purpose.** The purpose of LCMS is to reduce the operational and security human intelligence threat vulnerabilities by automated key management using electronically generated and distributed COMSEC key material. It is recommended that the LCMS Workstation be stored in an operational configuration where it does not have to be dismantled at the end of each workday. When this is not possible, the key generator and other classified components of the workstation must be secured in a GSA-approved security container.

**6.2.2 (U) LCMS Workstation.** The term "LCMS Workstation" specifically applies to the Local Management Device and Key Processor (LMD/KP). At a future date, the AKMS will include another component called the Automated Communications Engineering Software (ACES) workstation that can provide Signal Operation Instructions (SOI) and net planning information. This future capability will not be further addressed in this TB. The Army's distribution plan for LCMS Workstations placed a workstation in all existing Army COMSEC accounts, except for a few small Army COMSEC Accounts.

**6.2.3 (U) LCMS Functional Elements.** When the two functional elements of the LCMS Workstation are operating in tandem and interconnected, they are referred to as the LMD/KP. The LCMS Workstation consists of two functional elements.

**a. (U) First Functional Element.** The first functional element (LMD) is a commercial Pentium, (Y2K compliant) Personal Computer (PC), with a hard drive loaded with SCO UNIX and Local COMSEC Management Software (LCMS). Depending on the mission, units have been issued either a "ruggedized" laptop PC or a desktop model. When the PC is loaded with all the required software, it is referred to as a Local Management Device (LMD). If open classified storage of the LCMS Workstation is not possible, the LMD hard drive must be stored in a GSA-approved security container as specified in AR 380-5. The desktop model LMD's removable hard drive must be stored as SECRET collateral material. The laptop model's hard drive is not removable, which requires the secure storage of the computer itself, when required. The laptop LMD will also be stored as SECRET collateral material.

**b. (U) Second Functional Element.** The second functional area of the system is the Key Processor (KP). The KP must be stored in an approved COMSEC Facility except for those workstations that are deployed in a tactical environment for a period not to exceed 90 days.

**6.2.4 (U) LCMS Power Requirements.** The facility or work area housing the LCMS Workstation must have a continuous source of stable power. The use of a surge protector is recommended. An Uninterruptible Power Supply (UPS) is included with each initial fielding of the desktop LCMS Workstation to allow for an orderly and safe shutdown of the LCMS Workstation in the event of an unscheduled power loss. Due to the Laptop LMD's internal computer battery, an UPS is not provided for the Laptop configuration of the LCMS Workstation. It is recommended that the unit locally obtain an UPS for the protection and orderly shut down of the KP when in a laptop configuration.

## 6.3 ACCOUNTABILITY OF THE LCMS WORKSTATION.

(U) The LMD is an unclassified PC and must be accounted for on the unit property book and controlled by the Property Book Officer (PBO), IAW AR 710-2. The LCMS is classified SECRET (non-COMSEC accountable) and, when loaded onto the LMD, causes the hard drive of the LMD to be classified SECRET (not CMCS accountable). The removable hard drives and laptop LMDs with internal hard drives are to be controlled as SECRET collateral material as specified in AR 380-5. The KP is a SECRET COMSEC device and is centrally accountable in the CMCS as ALC-1 (Serial Number accountable to the COR). The KP is **not, repeat, *not*,** a Controlled Cryptographic Item (CCI).

## 6.4 INVENTORY REQUIREMENTS.

(U) Upon initial start up of an LCMS Workstation, COMSEC Custodians will print SF 153 hard copies of the following transactions as they occur. These documents will be retained as required by AR 380-40, Appendix C.

**a.** (U) Receipts for COMSEC Transactions.

**b.** (U) Incoming/Outgoing Transfer Reports.

**c.** (U) Reportable Destructions

**d.** (U) Local Destructions

**e.** (U) Active Hand Receipts

**f.** (U) Generation Reports

**g.** (U) Possession Reports

**h.** (U) Relief from Accountability Reports

**i.** (U) ALC 4/7 Inventory Reports (included in full local inventory). These reports are required so the auditors can verify that local inventories of ALC 4/7 material are being conducted. ALC 4/7 material, listed on a Relief from Accountability Report SF-153 is exempt from this requirement.

**6.4.1 (U) COMSEC Account Semiannual Inventory Report (SAIR).** For AKMS accounts, the COR electronically initiates a request for an SAIR to the LCMS Workstation. The COMSEC Custodian generates and forwards this inventory back to the COR within the required 30 days (45 days for National Guard and Army Reserve accounts only). Any AKMS-required modifications to the COMSEC Account Registration Packet (CARP) must also be forwarded to the Army service authority representative (CSLA). After the Central Office of Record (COR) reconciles the SAIR, a Certificate of Verification will be provided to the COMSEC Custodian via a Tier 1 free-form text message advising the commander that the assets charged to their COMSEC account have been satisfactorily accounted for.

**6.4.2 (U) COMSEC Account Change of Custodian Inventory Report (CCIR).** The CCIR for AKMS accounts will be created and sent by the custodian to the COR for reconciliation. The Service Authority **must** receive the CARP within 14 days after the CCIR has been sent. A new hard copy CARP, with an original wet signature, will be provided to the Service Authority for update of the database. A copy of the inventory with an original signature will also be maintained by the account. After the COR reconciles the CCIR, a verification that the account has been cleared will be provided to the

custodian via a free-form text message. The outgoing custodian **will not** be released from or depart the organization until this verification message is received. The account will print a copy of the message and file it with the original, signed inventory. The new custodian will not be capable of logging onto the LCMS Workstation and signing for any COMSEC material received by the account prior to his or her official appointment and issuance of the registration certification specified in the new CARP. After the appointment date and signature of the CCIR Certification & Correction (C&C) page, the new custodian will assume responsibility for all material and account records in their existing condition. **If the commander allows the COMSEC Custodian to depart the unit prior to clearance from COR, the commander assumes personal responsibility for the COMSEC account and any accounting irregularities that may exist.** A CCIR also serves as an SAIR. The next SAIR will be scheduled six (6) months from the CCIR signature date.

**6.4.3 (U) Special Inventory Report (SIR).** There are no Special Inventory Reports (SIRs) generated by the LCMS. Under circumstances other than a routine CCIR or SAIR, the need may arise for a custodian to perform an SIR. An example of an SIR would be an unexplained temporary absence or permanent and unauthorized absence of a COMSEC Custodian (see Table 6-2 for deletion of a user account from the LCMS). When an SIR becomes necessary, custodians will generate a CCIR, annotate that this is an SIR in the comment section (see paragraph 2.8, paragraph C, sub-paragraph 1), print the SF 153, pen and ink change the type of inventory from CCIR to SIR, and provide this report to the servicing COR.

**6.4.4 (U) Change of Account Location Inventory Report.** When an LCMS Workstation is to be physically relocated to another location, the custodian will perform the following:

**a. (U)** Generate a Change Account Location Inventory in the LCMS.

**b. (U)** Perform a 100% physical inventory of the COMSEC material being accounted for on the LCMS Workstation and any physical material on-hand prior to the movement, and verify this inventory upon arrival at the new location.

**c. (U)** If a COMSEC account is relocated to an area where an existing account does not exist, the following actions must be adhered to prior to movement of the AKMS account.

(1) (U) A new CFAR and CARP must be submitted to the COR. The COMSEC account number or EKMS ID will remain unchanged. Failure to obtain a new CFA prior to relocation will result in a reportable incident for all COMSEC material charged to the account.

(2) (U) Upon approval of the CFA, all COMSEC accountable material must be shipped via DCS or a properly cleared courier to the new, approved COMSEC Facility.

(3) (U) The CIK associated with the key processor must be transported in separate containers from the KP when being transported via DCS or via courier.

(4) (U) The LMD removable hard drive must be handled as SECRET collateral. All non-CMCS accountable material associated with the LMD must be shipped to the new location IAW AR 380-5.

**6.4.5 (U) AKMS Daily and Shift Change Inventory Requirements.** All Army COMSEC Accounts will conduct daily or shift change inventories as specified in paragraph 4.12, sub-paragraphs c and d. The LCMS does not provide a daily/shift change inventory sheet. Custodians will use a DA Form 2653-E or develop their own by use of word processor or spreadsheet.

**6.4.6 (U) ALC 4 Inventory Requirements.** AKMS cannot produce or print an inventory report for ALC 4 materiel only, as required in paragraph 4.13.5. To ensure that ALC 4 annual inventories are conducted and reported, custodians will print a copy of the Semiannual Inventory Report (SAIR) (created for the Local Account—not for the COR). The custodian will then inventory the ALC 4 material to ensure that all items are on-hand, line through the semiannual report, and make a pen and ink change stating “Annual ALC 4 Inventory.”

Table 6-1. Inventory Reports (AKMS Accounts)

| SITUATION | TIME OF SUBMISSION | COPIES | DISTRIBUTION | REMARKS |
|---|---|---|---|---|
| Semiannual Inventory (SAIR). | (1) The COR will initiate the inventory request.<br>(2) The account will conduct an inventory of reportable assets and return the C&C page within 30 days, electronically. | 2 | 1 COR<br>1 File | Monitored response by the COR until receipt of the inventory. |
| Change of Custodian Inventory Report (CCIR). | (1) Generated by COMSEC Account. Sent to the COR for reconciliation.<br>(2) The account will conduct an inventory and return the C&C page electronically and by hard copy immediately after the inventory, but NTE 45 days. | 2 | 1 COR<br>1 File | Tier 2 forwards the signed copy of the C&C page to the COR and retains one copy for file. |
| Special Inventory – Manual Change of Custodian Report. | Immediately after inventory. | 2 | 1 COR<br>1 File | Upon sudden and unexplained departure of custodian.<br>Tier 2 holds original signature copy. |
| Change Account Location Inventory-Movement or Deployment of a unit to another geographic area. | Immediately prior to departure and after arrival at destination. | 1 | | Notify COR of deployment |
| Conversion Report | Immediately after adjustment. | 2 | 1 COR<br>1 File | Used to report change of short title or serial number of material or equipment/ component conversion from one configuration to another and ALC changes. |
| Special Possession Report - COMSEC material recovered that had previously been deleted from accountability. | Immediately after recovery. | 2 | 1 COR<br>1 File | Indicate circumstances involved. An example would be inadvertent destruction of material. |
| Special Possession Report – COMSEC material found which is not on accounting records (SF 153). | Immediately after discovery. | 2 | 1 COR<br>1 File | Indicate circumstances involved. An example would be equipment found on-station. Depending on the circumstances, this may require a COMSEC Incident Investigation and Report. |



FOR OFFICIAL USE ONLY

## 6.5 LOCAL ACCOUNTING FOR COMSEC MATERIAL.

(U) This paragraph identifies *unique* COMSEC accounting procedures that must be implemented to ensure that AKMS COMSEC accounts adhere to COMSEC accounting policy outlined in AR 380-40 and Army COMSEC procedures outlined throughout this TB.

**6.5.1 (U) Hand Receipts (HR).** When it is required to provide COMSEC material for a specific or indefinite period of time, the material will normally be hand-receipted using an SF 153 generated by the LMD/KP. The material will only be hand-receipted to an individual. Within the AKMS, a Hand Receipt Holder (HRH) is registered as a Local Element. The HRH that takes possession of the material assumes direct responsibility for safeguarding this material.

**a. (U) Manual HRs.** Under unusual conditions (e.g., conditions that may delay a tactical mission), hand receipts may be prepared manually. See paragraph 4.11.3 for instructions on the preparation of a manual hand receipt.

**b. (U) HR Briefs.** The COMSEC Custodian will ensure all HRHs are properly briefed on the safeguarding, destruction, inventory and operating instructions for COMSEC material that will be in their possession. HRHs will sign a briefing statement prepared by the custodian attesting that they have been properly briefed on the responsibilities of an HRH. If material is to be sub-hand-receipted, the custodian must provide written approval to the sub-HRH.

**c. (U) HR Accountable Summaries.** Prior to taking possession of any COMSEC material, the COMSEC Custodian will process, print and distribute a Local Element accountable item summary that identifies all assets that will be signed for by the HRH. If there is an existing Local Element (an HRH account) the incoming HRH and outgoing HRH will perform a joint inventory to ensure all material identified in the accountable inventory is on hand.

**d. (U) HRH Material Transfer.** When the COMSEC Custodian has been notified that the hand receipt is ready for transfer, he or she will modify the current HRH (Local Element) registration data to reflect the incoming HRH's name and then process a local CCIR. The COMSEC Custodian will include comments explaining that this is a change of HRH, the date the joint inventory was completed, and any additional information deemed necessary. The COMSEC Custodian will print this inventory and perform a pen and ink change to the inventory type (i.e., Change of Custodian to Change of Hand Receipt Holder). The new HRH will compare the inventory report to the accountable items summary that was used to inventory: if there are no discrepancies, the new HRH will sign this Change of HRH Inventory. The Change of HRH Inventory will not be provided to the COR.

**e. (U) HRH Discrepancies.** If there are discrepancies, the new HRH will annotate them on the Change of HRH Inventory. It will be the outgoing HRH's responsibility to resolve all annotated discrepancies prior to departure from the unit and before changing the Local Element registration.

**6.5.2 (U) Inventory Maintenance.** An alternate HRH must also sign the Change of HRH Inventory if TOP SECRET material is currently on hand receipt or when such material is received. The issuing COMSEC Custodian will keep the original signed copy of the Change of HRH Inventory. A copy will be maintained by the current HRH. A hand receipt file will be maintained by both the issuing COMSEC account and the HRH. These hand receipt files serve as the record of accountability and responsibility for all material issued on hand receipt. Upon return of the material to the AKMS COMSEC account, the original copy of the hand receipt will be removed from the file by the custodian and returned to the HRH. Identification and disposition of hand receipt files will be IAW AR 380-40, Appendix C.

**6.5.3 (U) Accounting for Superseded Key.** The servicing COR for Tier 1 will automatically delete all regularly superseded key from the account assets on the supersession date assigned to this material. The material will continue to be reflected on the COMSEC account (Tier 2) local assets. When regularly superseded key reaches its supersession date, the COMSEC Custodian will perform a local destruction of the material. This **will not** be reported to the COR. LCMS does not allow for the custodian to destroy "electronic" key if the database reflects that a copy of that key is still

on hand receipt to a user. The COMSEC Custodian must ensure that users provide timely destruction reports.

**6.5.4 (U) Issue of ALC 4 Material Within AKMS.** In AKMS, issuing ALC 4 Material is not a valid transaction; however, the COMSEC Custodian performing the following two transactions can accommodate it:

**a. (U)** A hand receipt to the Local Element for the ALC 4 material will be performed between the custodian and the HRH. The SF 153 hand receipt block will be marked through and the "other" block will be annotated manually to reflect an "issue." The custodian will insert the following statement in the comment section of the hand receipt or on another sheet of paper that will be attached to this SF 153: "THE MATERIAL LISTED ABOVE HAS BEEN DROPPED FROM CMCS ACCOUNTABILITY AND HAS BEEN ISSUED TO YOU AS THE HRH. YOU ARE RESPONSIBLE FOR THE PROPER STORAGE, HANDLING, INVENTORY, AND DESTRUCTION OF THIS CLASSIFIED MATERIAL IAW 380-40." Local destruction records are required for all ALC 4 material marked "CRYPTO" regardless of the classification. These destruction records will be maintained for a period of 90 days. After the HRH has signed for this material, the custodian is no longer responsible. The HRH will sign the SF 153 and provide the original copy to the issuing COMSEC Custodian.

**b. (U)** Once the issue of ALC 4 material has been completed, the ALC 4 material needs to be removed from the LCMS database. The custodian will utilize "Destruction of Local Material" in LCMS to accomplish this. Custodians will annotate the SF 153 with the following statement either electronically or on a separate sheet of paper that will be affixed to the original destruction report: "THIS IS NOT A DESTRUCTION REPORT. THIS IS A RECORD OF THE ISSUANCE OF ALC 4 COMSEC MATERIAL TO AN AUTHORIZED USER. BY SIGNING THIS REPORT YOU ARE ASSUMING FULL RESPONSIBILITY FOR THE PROTECTION, DISTRIBUTION AND DESTRUCTION OF THIS MATERIAL." The custodian will print and retain a copy of this destruction report. To complete this transaction in the LCMS database, you must "confirm destruction of local material."

**6.5.5 (U) Clearing Typographical Errors When Entering a Physical Receipt into LCMS.** The following procedures must be followed to correct a transaction when a typographical error has been entered into LCMS:

Select accounting > possession > set material to pending investigation > select the short title to be corrected by highlighting it > right click, hold, and drag down to "material to be marked" box > release the right click and the material should automatically show up > select "edit quantities" > the next screen appears, highlight the short title and in the "qty to mark" box, type in the number of items to mark (usually 1, unless you entered a quantity of more than one when you entered the short title) > select "update" and select "mark items" > select exit on the "set material to pending investigation" screen > select accounting > relief from accountability report > originate relief from accountability report, on the "quantity selection screen" in the top box "reference for reporting relief from accountability," enter the reason for requesting relief from accountability (i.e., "MATERIAL INCORRECTLY ENTERED INTO LCMS DATABASE") > click on the short title in the window > click on the "qty to relieve" and enter the number to relieve and click "update" > select "prepare report": if remarks are desired, enter them and any comments > select "record annotations" wrap and send the report to the servicing COR.

**6.5.6 (U) Recording STU-III Key Conversions in AKMS.** When converting STU-III in AKMS, the key must be issued to a HRH. As explained earlier in this document, an HRH (Local Element) must be an individual. The HRH may be either an appointed subordinate if the account is responsible for keying the STU-III, or an HRH from another section within the unit/command. Once the key has been loaded into the STU-III, the Crypto Ignition Key (CIK) log must be completed and returned to the issuing custodian. The custodian will enter the transaction as "filled-in end equipment" in LCMS. Upon receipt of the conversion notice from the Central Facility, file the conversion notice in the COMSEC accounting files. Re-key is not entered into the LCMS Workstation.

**6.5.7 (U) Five Digit Outgoing Voucher Number.** When physical material is received by an AKMS COMSEC account and the "reconcile physical material hardcopy" report is created, LCMS can only accept a maximum of five (5) digits as input for the incoming voucher number. In cases where the voucher number is longer than 5 digits, custodians should enter the last five digits of the voucher number as the incoming number.

**6.5.8 (U) Destruction "Certification Statements"** IAW TB 380-41, paragraph 4.19.5b, the "I certify" statement must be inserted on all consolidated destruction reports. In LCMS, it will not be required to insert the "I certify" statement. All reportable destruction reports generated by LCMS are "consolidated" destructions. Custodians will retain the local vouchers with wet signatures and post with their reportable destruction report.

**6.5.9 (U) Inadvertent Destruction of COMSEC Material.** Due to the strict security procedures enforced within the LCMS Workstation, when destruction of material is erroneously entered into AKMS, LCMS cannot "reverse" this action. Should this situation occur, the custodian must perform the following steps immediately:

**a. (U)** Contact the COR account manager via e-mail, message, or fax with an explanation of the error (include the short title, edition, quantity, and serial number). Prepare a Memorandum For Record (MFR) explaining the circumstances of the error.

**b. (U)** Within LCMS, the custodian will generate a "reportable destruction report," annotate what transpired in the comment section, print and retain the document as an accountable record, and send the destruction report via the message server to the COR.

**c. (U)** Contact the EKMS Help Desk, explain the situation, and ask to be walked through Inventory Reconciliation Status Transaction (IRST) or inventory cycle procedures.

**d. (U)** The custodian will then be required to add those items back into the LCMS database. The custodian should click on accounting > possession > originate possession report. In the "reason for possession" box, enter what transpired, enter the item, and then click "add." Prepare the report and record annotations. These steps will cause a "Possession Report" to be generated. The custodian must wrap and send the transaction to the COR. A copy of the Possession Report will be printed, attached to the copy of the reportable destruction report and the MFR, and retained on file. When the item is later destroyed, normal destruction procedures will be followed.

**6.5.10 (U) Account Transactions to COR.** When requested, the custodian will retransmit transactions to the COR. In the event that the COMSEC account transactions have been archived, the COR will be provided a hard copy of the transaction and will be notified that requested soft copy of these transactions have been archived.

## 6.6 GENERAL INFORMATION ON AKMS ELECTRONIC KEY DISTRIBUTION AND DESTRUCTION.

(U) The following paragraph provides some general guidance/information on AKMS electronic key distribution and destruction.

**6.6.1 (U) Electronic Key Distribution.**

**a. (U)** AKMS COMSEC accounts will issue electronic keying material to Hand Receipt Holders (HRHs) via a Data Transfer Device (DTD) or to a Common Fill Device (CFD). The COMSEC Custodian will retain a signed copy of the issuing SF 153 until a destruction certificate is received from the user or until unused portions of the electronic key is returned from the HRH. An automated audit trail exists when material is distributed to a DTD. The HRH can verify if key was received by viewing the key storage register in the DTD. The COMSEC Custodian will attach a descriptive ID to all electronic keying material being distributed to the DTD. This ID will provide a quick, verifiable means to identify the material.

**b. (U)** It may become necessary to distribute the electronic keying material below the hand receipt level, or sub-hand receipt. This will be accomplished by issuing the key from DTD to DTD, DTD to CFD, or CFD to CFD. HRHs will prepare a local Electronic Key Management (EKM) worksheet to record or control distribution (custodians may create their own EKM worksheets as long as the required fields are inserted): see Appendix D for a sample (reproducible) worksheet. The HRH will retain the local record until destruction and/or turn-in has been completed and the COMSEC Custodian closes out the hand receipt.

**6.6.2 (U) Electronic Key Destruction.** To ensure 100% accountability and control of electronic keying material from its generation until destruction, COMSEC Custodians and users must document a positive and uninterrupted audit trail. The HRH and a witness shall verify the destruction by signing and returning a Local Destruction Report to the issuing COMSEC Custodian. Signed Local Destruction Reports will be retained by the custodian as supporting documentation for the consolidated (reportable) destruction report IAW TB 380-41, and filed IAW AR 380-40, Appendix C. When HRHs distribute electronic key below the hand receipt level, they must ensure this material is destroyed upon supersession and that a valid, written audit trail of the destruction is completed and retained on-site. A locally developed EKM worksheet will be used to track this destruction. The HRH will retain a copy of the Sub-Hand Receipt Holder's EKM worksheet for 60 days after the key is destroyed or turned in to the custodian.

## 6.7 ACCESSIBILITY TO THE LMD/KP.

(U) All personnel having read/write access to the LMD/KP will be registered as a *User*. The Systems Administrator (SA) for the LCMS Workstation will assign appropriate privileges for each individual. When there is a permanent, unauthorized absence of a COMSEC Custodian or alternate having access to the LMD/KP, or if an individual is no longer authorized access, the individual will immediately be deleted from the LCMS Workstation (see Table 6-2).

**6.7.1 (U) CIK and PIN Number Storage.** The operator Cryptographic Ignition Key (CIK) and Personal Identification Number (PIN) for the LCMS Workstation may be stored together unless the account is a TOP SECRET (TS) account. If the account is a TS account, follow the procedures set forth in AR 380-5, chapters 6 & 7.

**6.7.2 (U) LMD/KP "Disaster Recovery Kit."** The following is a list of critical materials (as a minimum) that must be maintained by each COMSEC account in case the LMD/KP has failed and must be reinitialized. The following listing is referred to as a "Disaster Recovery Kit."

**a. (U)** KP REINIT CIK #1 (2 each), KP REINIT CIK #2 (2 each). One set of the KP REINIT CIKs should be hand-receipted to the unit security office. The other set will remain with the Disaster Recovery Kit.

**b. (U)** Backup KP User CIKs, one each for the primary and alternate custodian, will be created and maintained in the Disaster Recovery Kit.

**c. (U)** A minimum of two EKMS ID STU-III keys must be retained on hand.

**d. (U)** The u/ Filesystem Backup Tape (as a minimum, the current day or a tape for the previous day).

**e. (U)** LMD User's Floppy Disk (1 each, created and updated by custodian).

**f. (U)** SCO UNIX Emergency Floppy Disk - boot (1 each)

**g. (U)** SCO UNIX Emergency Floppy Disk - root (1 each)

**h. (U)** SCO UNIX OPENSERVER 5.0.5 Desktop Installation Software CD (1 each).

**i. (U)** SCO UNIX OPENSERVER 5 Supplement CD (1 each).

**j. (U)** Floppy disk, SCO OPENSERVER 5 OSS497B or OSS497C Patch (1 each).

**k. (U)** KP MPUP Field Download 0403.

**l. (U)** Master Copy of Utility Floppy Disk (UFD) (1 each).

**m. (U)** LCMS 4.03 Installation CD (1 each).

**n. (U)** (Laptop ONLY): LynnSoft PC Card Software, lsio4ports, Part # LSPC5D, Version 2.0 Release 1.6 (1 each).

**o. (U)** Floppy Disk (Laptop only): LynnSoft PC Card Software, LSIO4PORTS, part # LSPC5D, Version 2.0, Release 1.6 (1 each).

**p. (U)** LCMS Workstation System Backup and Restore Procedures for Phase 4 (1 each) (available in the SA Manual).

**q. (U)** (Desktop ONLY): Key to the mounting lock on the removable hard drive chassis (1 each).

**r. (U** (Desktop ONLY): Key to the rear CPU cabinet lock (1 each).

**s. (U)** SCO OPENSERVER 5 Certificate of License and Authenticity (COLA) should be maintained by the COMSEC account. If the Information Assurance Security Officer (IASO) requires that the original COLA be stored in the IASO office, arrangements to obtain this COLA within 24 hours must be made with the IASO.

**(U) The LCMS Workstation Disaster Recovery Kit** is mission essential and must be maintained as a complete unit to ensure immediate recovery of the system. It cannot be emphasized enough that material comprising the Disaster Recovery Kit must be maintained. **Failure to maintain the complete recovery kit will be considered a COMSEC Incident and will be reported to the Army COMSEC Incident monitoring activity**.

**6.7.3 (U) Archiving and Key Processor (KP) Changeover.** Archiving and KP changeovers of the LCMS Workstation must be performed quarterly. More frequent archiving is acceptable and encouraged for accounts that process numerous transactions. To ensure that information does not become lost and the LCMS system does not become overloaded with information, a database backup of the system must be performed. The custodian must perform the changeover in the following order:

**a. (U)** A backup of the /u filesystem must be performed using the UFD Backup and Restore menu option #2.

**b. (U)** Once the /u filesystem back up has been completed, archiving of the LCMS database will be performed. Archiving will remove all completed transactions that have occurred on the system to date. It is recommended that archiving be performed on a floppy disk due to the smaller size of the disk and the cost effectiveness; however, any removable storage device may be used. Each time the system is archived, a different diskette/ storage device must be used. This will prevent the information from being overwritten and lost.

**c. (U)** Next, the custodian will perform the KP changeover. The KP changeover involves decrypting and re-encrypting all key and voucher data in the LCMS database. Archiving must be performed prior to KP changeovers. This procedure will minimize the amount of time required to decrypt and re-encrypt data stored in the LCMS database. A new set of REINIT #2 keys will be created at the end of this process; therefore, there must be 2 blank KSD-64s on hand for this purpose. DO NOT ZEROIZE THE OLD REINIT KEY! The two most current sets of REINIT keys must be kept on hand. Any REINIT keys older than the two most current sets can be zeroized.

**d. (U)** Once it is determined that the KP changeover has been effectively accomplished, a /u filesystem backup must be performed again at this point. This will complete the functions that are required to ensure that the post-KP changeover LCMS database is successfully backed up. This /u filesystem backup may be done on the same tape as the first one mentioned in subparagraph a. All backup and archiving media must be marked SECRET and safeguarded according to AR 380-5. For additional backup requirements, refer to NAG-71. Explanations of archiving and changeover are contained in the EKMS 704 series user's manual. COMSEC Custodians may also refer to guidance received from CSLA, such as the Utility Floppy Disk, and specific Army Backup and Restore Procedures documentation contained in the Army Phase 4 LCMS Workstation System Administration Manual (TB 11-7010-348-10-1).

**6.7.4 (U) Accountability for KSD-64 Transit CIKS.** Transit CIKs that are fielded with a new depot-initialized KP are ALC- 4 and will be accounted for in the CMCS until the KP is initialized within LCMS. This transit CIK then

becomes the user's CIK and will be handled as SECRET "collateral" material. The CIK will no longer be accountable in the CMCS. Whenever a newly initialized KP is provided to an account, it is the responsibility of the account to provide blank KSDs.

**6.7.5 (U) AKMS KP Settings.** When an account is fielded via an LCMS Workstation, the KP settings are established. The KP selection in the local account registration must remain *"on"* at all times. De-selecting the KP option in an attempt to increase the processing times of the LCMS is a reportable COMSEC Incident.

**6.7.6 (U) AKMS User Deletion.** See Table 6.2.

## Table 6-2. Deletion of an AKMS User Account from an LCMS Workstation

| *This procedure was developed using an LCMS Workstation running SCO OpenServer 5.0.5 Desktop and LCMS 2.0.2.2.* | | |
|---|---|---|
| | **Step** | **Action** |
| | 1 | You must be logged into LCMS as a user ID-privileged as an LMD Administrator. If the account ID you are about to delete has been tagged as a KP operator or KP administrator, you will need to be logged onto the KP before you can delete the user ID from LCMS. |
| | 2 | From the LCMS Desktop Menu Bar, click on *Registration*. In the *Operator Tool* window that opens, click on *Operator Tool*. |
| | 3 | In the *Operator Tool* window, click on the line containing the user ID that is to be deleted. This will highlight the line in reverse video. Then, click on the *Delete* button. In the *Operator Delete Confirmation* window that opens, click on the *Continue* button. |
| | 4 | If the user ID being deleted is associated with the KP, you will need to respond to several prompts on the KP display. Answer the KP questions by pressing the appropriate button on the KP. |
| | 5 | After a few seconds, confirm that the user ID no longer displays in the *Operator Tool* window. In the same window, click on the *Exit* button. |
| | 6 | Simultaneously depress the keys <Ctrl><Alt><F1> to switch to screen 1, the Console screen. |
| | 7 | Log in as root. |
| | 8 | Use the UFD Utility Menu option #2 to remove the user ID from UNIX and to remove that user's home directory from the system. Proper procedure requires that the System Administrator review the content of the user's home directory before deleting its content. |
| | 9 | If the person using the now deleted user ID had knowledge of the root's password, the password for root must be changed. To change the root's password, use the following command and answer its prompts in accordance with current security guidelines:<br>passwd <Enter> |



FOR OFFICIAL USE ONLY

## 6.8 STORAGE OF LCMS WORKSTATION.

(U) Any space housing the LCMS Workstation must be an approved COMSEC Facility, except for a workstation deployed in a temporary environment for a period not to exceed 90 days. It is recommended, that the LCMS Workstation be stored at all times in its operational configuration, in a secure area approved by the command's cognizant security authority for the open storage of SECRET material. If open storage in an approved COMSEC Facility is not possible, the LMD hard drive and key processor associated with the desktop, and the complete laptop LMD must be stored in a GSA-approved security container when unattended, as specified in AR 380-40. Frequent disassembly and removal of this sensitive equipment for storage, and subsequent reinstallation, can be expected to significantly reduce its serviceable life expectancy. Extreme care must always be exercised when handling the equipment and when connecting/disconnecting the LMD/KP to prevent damage to external connectors. Open storage requirements for SECRET material are outlined in AR 380-5.

## 6.9 ASSOCIATED EQUIPMENT AND REQUIREMENTS.

(U) All COMSEC accounts receiving the LCMS Workstation **must, repeat, *must*** have a dedicated STU-III. The STU-III will be used for connection into the AKMS, and will require the use of a special COMSEC key, which is provided by CSLA during AKMS fielding. The STU-III associated with AKMS can be used to make other secure calls, but it must be available to the AKMS terminal at all times in order to provide continuous key management and distribution functions, as well as connection into the AKMS architecture, as needed.

**6.9.1 (U) STU-III Connectivity**. The AKMS requires STU-III connectivity to a message server. AKMS message servers are located at the Primary Tier 1 Sites (PT1S) (i.e., the CORs located at Ft Huachuca, AZ; San Antonio, TX; and the Extension Tier 1 site located in Mannheim, Germany). The location of the message servers supporting Army COMSEC accounts will vary. Commanders should consider upgrading existing telephone lines supporting Army COMSEC accounts based on this requirement. The use of operator-assisted calls is not conducive to efficient automated operations and may jeopardize the successful completion of AKMS transactions between the LCMS Workstation and the PT1S message servers during critical periods of operation.

**6.9.2 (U) Laser Printers**. All accounts receiving LCMS Workstations will be fielded with dedicated laser printers. If, for some reason, this printer becomes defective and it is necessary to use a replacement laser printer, it must be the HP LaserJet III or equivalent. If the account uses a dot matrix printer, it must be the Epson LQ-570 or compatible. There are some restrictions with respect to using a dot matrix printer.

**a**. **(U)** Screen dumps will not print.

**b.** **(U)** Most of the activity reports will print out but the printout may not contain all the information because of the paper width.

**c.** **(U)** Activity reports will be printed only in landscape mode.

**d.** **(U)** All other printouts should work well, including the COMSEC Material Report (SF 153) and printable icon reports.

**6.9.3 (U) DTD**. A Data Transfer Device (DTD) must be on hand at each AKMS account.

**6.9.4 (U) Data Cartridge**. An HP T-20 Data Cartridge (nomenclature HP C 4435"X") is required for the LCMS to perform back-up operations. It is available in single pack (HP C 4435A), double pack (HP C 4435B), or five-pack (HP C 4435D). If there is any difficulty with the procurement of this item, see Appendix F of this TB for points of contact, or request assistance from the AKMS Help Desk.

## 6.10 TRAINING.

**(U)** Both the custodian and an alternate from each COMSEC account must be trained on the operations of the LCMS Workstation (see paragraph 2.7.1[c]). There must be a minimum of one System Administrator (SA) at each camp, post, and station that the commander will make available to perform SA duties with reference to the AKMS.

**6.10.1 (U) LCMS Operator Training Criteria**. Personnel selected for LCMS operator training must be appointed COMSEC Custodians and alternates. Custodians **must** have previously attended the Standardized COMSEC Custodian Course (SCCC). Personnel attending LCMS training must be computer literate and preferably have some knowledge of the UNIX operating system. It is imperative that trained individuals return to their units and provide training to the COMSEC account clerks and clerical personnel on the operations of the LCMS. Commanders must carefully consider local personnel transfers, separations and retirements to ensure that there are sufficient LCMS-trained personnel to occupy these critical positions.

## 6.11 LCMS MAINTENANCE.

**6.11.1 (U) LMD Accountability.** The LMD is accounted for on the unit property book. It will be maintained according to existing installation support procedures for the repair and service of classified automation systems.

**6.11.2 (U) Depot Level Repair.** The Key Processor (KP) is a SECRET, COMSEC device. Maintenance or repair of the KP below depot-level is not authorized. When failures of the KP occur, it must be evacuated through COMSEC account channels to Lackland AFB in San Antonio, TX, via Defense Courier Service (DCS). Every three (3) years the KP must be returned to San Antonio for scheduled maintenance. CSLA will monitor the distribution of the KP within the Army and alert COMSEC accounts when the KP must be returned for maintenance and re-certification. Commanders at all levels must stress proper care and handling of the KP. Misuse or damage of the KP, other than fair wear and tear, may result in a report of cursory investigational and substantial financial liabilities to the user.

**6.11.3 (U) Replacement KP.** Due to security considerations and because of anticipated battery failure within the KP, it is essential that, when CSLA notifies the account to evacuate the KP for scheduled maintenance, this action be taken in a timely manner. Replacement KP devices will be located at pre-positioned sites. When an account receives notification to return a KP to Lackland AFB, TX, for maintenance, a replacement KP will be automatically transferred to the account from the geographical area servicing the account. Once the new KP is received and key data transferred, the old KP must be zeroized. The custodian will then make arrangements to ship it via DCS in its specialized shipping container to the COMSEC Account at Lackland AFB, TX.

## 6.12 ADDITIONAL ARMY PUBLICATIONS.

**(U)** LCMS Workstations are fielded with the following reference publications:

- *EKMS 704C Volume 1 (LMD/KP Operator's Manual).
- *EKMS 704C Volume 2 (LMD/KP Quick Steps and Troubleshooting Guide).
- TB 11-7010-348-10-1 (Technical Bulletin System Administration Manual for Army Phase 4 Local COMSEC Management System [LCMS] Workstation).
- TB 11-7010-293-15-1 (Warranty Program for Army Key Management System [AKMS] AN/GYK-49[V]1&2).
- TM 11-7010-293-12 (Technical Manual Operator's and Unit Maintenance Manual, Computer Set, General).

* Indicates documentation provided in both hard copy and HTML format.

**6.12.1 (U) LMD Software Upgrade**. (U) As the LCMS Workstations are upgraded with new versions/phases of LCMS, the appropriate documentation in the preceding paragraph will also be updated. If the need exists to validate the current editions of AKMS manuals, users should contact the Army EKMS Help Desk.

**6.12.2 (U) Doctrine**. COMSEC accounts should have the following Army-adopted NSA doctrine and policy guides on hand:

- NAG 47 (Operational Security Doctrine for The AN/CYZ-10/10A Data Transfer Device [DTD]).
- NAG 71 (Operational Security Doctrine for The Local Management Device/Key Processor [LMD/KP]).

## 6-13 COMMUNICATIONS.

(U) The Public Telephone System Network (PTSN) dial-up system will provide communications between the LCMS Workstations and the EKMS message servers located at the Primary Tier 1 Sites. Army COMSEC accounts within the European Theater will have connectivity to the European Extension Tier 1 (ET1) site. This connectivity will be secured by either STU-III or STE secure voice and data telephone equipments. This configuration also allows for the distribution of electronic COMSEC keying between COMSEC user accounts (Tier 2 – Tier 2). The STU-III or STE interconnected to a DTD and interfaced through the PTSN provides the COMSEC account with the capability to provide electronic key material via direct communications from Tier 2 to Tier 3.

## 6-14 AKMS ACCOUNT INVENTORIES.

(U) ALC 7 material is locally generated electronic key. A printout of the ALC 7 material is required annually for the custodian's review. The custodian must ensure all superseded ALC 7 key material is destroyed upon supersession.

**THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY**

# CHAPTER 7

# COMSEC COMPROMISES AND INCIDENTS

## 7.1 COMPROMISES AND INCIDENTS.

(U) It is important that all personnel who possess, handle, operate, maintain, or repair COMSEC material be totally familiar with physical and cryptographic security policies and procedures. Personnel will report all security violations to the COMSEC Facility supervisor, the COMSEC Custodian, and the local commander. *An undetected or unreported incident is the most damaging security violation of all because the potential damage to national security cannot be neutralized.*

**(U) Any individual who knowingly conceals, obstructs, fraudulently alters records, or otherwise attempts to cover-up the existence of a COMSEC Incident, and any individual who becomes aware that a COMSEC Incident has occurred and fails to report such an incident, are both guilty of a criminal offense punishable under federal statute and the UCMJ, as applicable.**

**a. (U) Compromises.** A compromise results from any event or action where COMSEC material is irretrievably lost or available information clearly proves that unauthorized persons have gained access to classified COMSEC information or unclassified key marked "CRYPTO."

**b. (U) COMSEC Incident.** A COMSEC Incident is an occurrence that potentially jeopardizes the security of COMSEC material or the secure electrical transmission of national security information (see Table 7-1). AR 381-12 requires the local U.S. Army counterintelligence support unit be notified of all reportable COMSEC Incidents.

**c. (U)** There are four types of COMSEC Incidents that **must** be reported (reference Table 7-1 for a specified listing of each type of incident):

**(1) (U)** ***Physical Incidents.*** These include the loss, theft, loss of control, improper preparation of, or lack of preparation of, destruction reports (including back-up documentation for consolidated destruction reports) for COMSEC material; and the capture, recovery by salvage, tampering, or unauthorized viewing, access or photography of classified COMSEC material or unclassified key marked "CRYPTO." The loss, theft, capture, recovery by salvage, or tampering with a Controlled Cryptographic Item (CCI), keyed or un-keyed, is also considered a Physical COMSEC Incident and will be reported accordingly.

**(2)** ***(U) Personnel Incidents.*** Any attempted recruitment, known or suspected contact by a foreign intelligence entity, capture by the enemy, or unauthorized absence or defection of an individual having knowledge of and access to COMSEC information or material are considered Personnel Incidents. The unauthorized disclosure of COMSEC information, or attempts by unauthorized persons to affect such disclosure, also fall into this category.

**(3)** ***(U) Cryptographic Incidents.*** Any equipment malfunction, human error by an operator or COMSEC Custodian that adversely affects the cryptosecurity of a machine, auto-manual, or manual cryptosystem is a Cryptographic Incident. Unique incidents, which pertain to specific cryptosystems, are contained in technical cryptographic operational operating manuals (TM/KAO), maintenance manuals (KAM), limited maintenance manuals (LMM), technical bulletins (TB), or in specific DA pamphlets.

**(4)** ***Administrative Incidents.*** Any action that jeopardizes the *integrity* of COMSEC material is considered an Administrative Incident. These incidents include insecure practices that are dangerous to COMSEC security as well as violations of COMSEC procedures that require corrective action to ensure the violations do not recur.

Table 7-1. Reportable COMSEC Incidents

| TYPE OF INCIDENT | CIRCUMSTANCES (See AR 380-40 for additional information) |
|---|---|
| **1. Physical Incidents** ***(Reportable to the NSA and COR)*** | **a. Loss due to:**<br>1. Technical Surveillance.<br>2. Combat.<br>3. Capture.<br>4. Theft.<br>5. Other<br><br>**b. Physical security violations:**<br>1. Tampering.<br>2. Unauthorized viewing.<br>3. Recovery by salvage.<br>4. Photography of classified material or unclassified key marked "CRYPTO."<br>5. Material found that was previously reported lost.<br>6. COMSEC material left unsecured or unattended where unauthorized persons had access.<br>7. Transportation/shipment via unauthorized means.<br>8. Improper destruction.<br>9. Unauthorized maintenance or modification.<br>10. Deliberate falsification of COMSEC records or reports.<br>11. Unexplained removal of keying material from its protective packaging.<br>12. COMSEC material not accounted for on accounting records or COMSEC material on hand previously reported as destroyed.<br>13. Loss of TPI or No-Lone Zone for Top Secret (TS) material.<br>14. Any loss of control over a keyed common fill device.<br>15. Discovery of COMSEC material not completely destroyed and left unattended.<br>16. Discovery of a clandestine electronic surveillance or recording device in or near a COMSEC Facility.<br>17. Unexplained zeroization of COMSEC equipment when there are indications of unauthorized access or penetration.<br>18. Unauthorized copying or reproduction of COMSEC material.<br><br>**c. Any other occurrence jeopardizing the physical security of COMSEC material or information.**<br><br>**d. Loss, theft, capture, recovery by salvage, or tampering with keyed or un-keyed CCI equipment.** |



FOR OFFICIAL USE ONLY

Table 7-1. Reportable COMSEC Incidents (Continued)

| TYPE OF INCIDENT | CIRCUMSTANCES |
|---|---|
| **2. Cryptographic Incidents** ***(Reportable to the NSA and COR)*** | **a. Use of key material which has been:**<br>1. Compromised<br>2. Superseded<br>3. Defective<br>4. Previously used (not authorized for re-use)<br><br>**b. Incorrect application of key material:**<br>1. Use of key produced without authorization of the NSA (homemade maintenance, homemade codes, etc.).<br>2. Without authorization of the NSA for other than the intended purpose (test key for operational use; key used on more than one type of equipment). Does not include use of operational key for training when authorized by the CONAUTH.<br>3. Unauthorized extension of a cryptoperiod.<br><br>**c. Any equipment malfunction, operator or management error that adversely affects the operational security of a cryptosystem.**<br><br>**d. Use of COMSEC equipment with defective cryptologic circuitry or use of unapproved operating procedures.**<br><br>**e. Plain text transmission resulting from COMSEC equipment failure/malfunction.**<br>1. Transmission during a failure.<br>2. Transmission after an uncorrected failure that may cause improper operation of COMSEC equipment.<br>3. Operational use of COMSEC equipment without completion of alarm-check test or after failure of the required alarm-check.<br>4. Discussion via non-secure communications of the details of a COMSEC equipment failure or malfunction.<br><br>**f. Any other occurrence that may jeopardize the cryptosecurity of a COMSEC system.** |
| **3. Personnel Incidents** ***(Reportable to the NSA and COR)*** | **a. COMSEC personnel who are known or suspected of:**<br>1. Absence without leave.<br>2. Defection.<br>3. Espionage.<br>4. Treason.<br>5. Attempted recruitment.<br>6. Control by a hostile intelligence entity.<br>7. Capture by the enemy during hostilities.<br>8. Sabotage by a person having detailed knowledge of COMSEC information.<br>**b. Any other occurrence that may jeopardize the security of COMSEC material or the material it protects.** |

| Table 7-1. Reportable COMSEC Incidents (Continued) | |
|---|---|
| **TYPE OF INCIDENT** | **CIRCUMSTANCES** |
| **4. Administrative Incidents** ***(Reportable only within the Army chain-of-command as directed by the MACOM. At a minimum, the incident* must *be reported to the CONAUTH.)*** ***(For KOV-14 User Cards, see paragraph 7.9 of this TB)*** | **a. Actions which jeopardize the integrity of COMSEC material:**<br>1. Premature or out-of-sequence keying.<br>2. Inadvertent destruction of key material.<br>3. Destruction without authorization of CONAUTH.<br>4. Receipt of a package containing COMSEC material with a damaged outer wrapper, but the inner wrapper is intact.<br>5. Failure to zeroize a common fill device or failure to destroy COMSEC material within required time limits. (IAW AR 380-40 paragraph 7-3d[4], late destruction over 30 days is a Physical COMSEC Incident.)<br>6. Removal of key material from protective packing prior to issue or removal of protective packaging without authorization.<br>7. Failure of a user to properly safeguard or secure unclassified Cryptographic Ignition Keys (CIK), PCMCIA Cards, PKI Devices, Common Access Cards, etc.<br><br>**See DA Pamphlet 25-380-2 for reporting CCI Administrative Incidents.** |

**CAUTION: Comply with the following security tips:**

1. **(U) Restrict knowledge of information concerning tampering with COMSEC equipment, penetration of protective technologies, information related to system vulnerabilities, or discovery of clandestine devices on a strict <u>need-to-know</u> basis.**

2. **(U) Immediately and simultaneously report to the NSA, the local counter-intelligence field office, and the controlling authority when tampering is known or suspected. Wrap and seal the material along with all protective technologies and store it in the most secure limited-access area available. Take no action until instructions are received from the NSA.**

3. **(U) Where a clandestine surveillance or listening device is suspected, do not discuss it in the area of the device or anywhere else a device may similarly have been installed. Take no action that might alert the clandestine activity, except on instructions from the applicable counter-intelligence field office or the NSA.**

## 7.2 REPORTING COMSEC INCIDENTS.

**a. (U)** In accordance with AR 381-12, the local U.S. Army Counterintelligence Support Unit will be notified of all reportable COMSEC Incidents immediately (the same day) upon discovery. Formal written reports, as directed in this TB, are required within 24 to 72 hours depending on the type of incident (see paragraph 7.3 below).

**b. (U)** The U.S. Army CECOM Communications Security Logistics Activity (USACSLA) is designated by HQDA as the Army COMSEC Incident Monitoring Activity (CIMA) and the Adjudication Authority for all reportable COMSEC Incidents. CSLA will be an addressee on all incident reports. For assistance and guidance in the preparation and submission of incident reports, contact the COMSEC Incidents Program Manager at Commercial (520) 538-6008/ DSN 879-6008 or via e-mail at: <u>incidentdesk@csla.army.mil</u> or <u>incidentdesk@huachuca-emh99.army.smil.mil</u>.

**7.2.1 Responsibilities.**

**a. (U)** The NSA will perform the following functions:

(1) (U) Evaluate all Cryptographic and Personnel COMSEC Incident Reports.

(2) (U) Evaluate all Physical COMSEC Incident Reports involving keying material **when the responsible Controlling Authority cannot be identified.**

(3) (U) Evaluate all Physical COMSEC Incidents **involving multiple Controlling Authorities of different departments or agencies.**

(4) (U) Evaluate all COMSEC Incidents involving the Secure Data Network System (SDNS) and STU-III Key.

(5) (U) Evaluate all reportable COMSEC Incidents related to:

(a) (U) Tampering, sabotage, or evidence of covert penetration of packaging.

(b) (U) Unauthorized modification of COMSEC equipment, security containers, or vaults where COMSEC material is stored.

(c) (U) Unauthorized access to classified COMSEC technical material promulgated by the NSA (e.g., algorithms, logic, KAMs, technical engineering documents).

**b. (U)** The Army CIMA will perform the following measures:

(1) (U) Establish a formal register to assign case numbers and a records jacket for all reportable COMSEC Incidents. All records and supporting documents will be retained on file for not more than six (6) years or until no longer needed following the completion and closure of the case file (reference AR 380-40 for additional information).

(2) (U) Immediately report the following types of COMSEC Incidents to HQDA, G-2, ATTN: DAMI-CDS.

(a) (U) Loss or theft of Mission/Inter-theater COMSEC Package (ICP) key.

(b) (U) Falsification of records that result in a compromise of COMSEC material.

(c) (U) Any incident that, in the opinion of the Controlling Authority and/or CIMA Program Manager, may adversely impact mission critical command, control, and communications (C3), sensitive intelligence activities, or ongoing contingency operations.

(3) (U) Evaluate Physical COMSEC Incidents involving multiple Army Controlling Authorities.

(4) (U) Evaluate Physical COMSEC Incidents involving a single Army Controlling Authority **when that Controlling Authority caused the incident.**

(5) (U) Direct additional investigation and reporting, as warranted.

(6) (U) Administer final adjudication to determine when a reported COMSEC Incident has resulted in a COMSEC Insecurity.

(7) (U) Provide statistical data and a narrative assessment on the number and type of reportable COMSEC Incidents for inclusion in the CSLA Annual COMSEC Assessment Report to HQDA per AR 380-40, paragraph 6-4.

**c. (U)** Controlling Authorities will be responsible for the following:

(1) (U) Evaluate Physical COMSEC Incidents involving keying material they control, except as noted in subparagraph b above.

(2) (U) Notify the Army CIMA and the NSA regarding the results of all completed evaluations.

(3) (U) Initiate recovery actions when it is believed that material has been compromised. See AR 380-40, paragraph 7-10.

(4) (U) Evaluate and report incidents involving Signal Operating Instruction (SOI) as classified information under the provisions of AR 380-5.

**7.2.2 Controlling Authority Limitations.**

(U) Controlling Authority responsibilities are limited to initiating precautionary supersession and recovery actions, as warranted, and rendering an evaluation as part of the administrative processing and closure of the Incident. **Recommendations related to procedural changes or disciplinary measures are outside the scope of this responsibility.**

## 7.3 COMSEC INCIDENT REPORTS.

**7.3.1 (U) Report Contents.** (See following sub-paragraphs 7.5, 7.6, and 7.7 for detailed instructions.)

**a. (U)** In order to conduct a proper evaluation, it is vital that all immediately available and essential information be included in Initial Reports concerning reportable COMSEC Incidents. Incident reports must NOT be delayed in order to obtain additional information. For example, a missing current key list will be reported immediately after a reasonable search.

**b. (U)** Incident reports will be classified according to content and must be transmitted by appropriate electrical means. Memorandum reports may be used only when electrical means are not available. COMSEC Incident Reports do not require the assignment of a Reports Control Symbol (RCS).

**7.3.2 (U) Reporting Incidents.** Reports are normally filed in sequence, each subsequent report relaying additional information, as the incident investigation proceeds. The particular nature of each incident will determine the precedence and the allowed preparation time for an incident report. There are four types of reports:

***a. (U) Initial Report***. This report is required for each detected COMSEC Incident. The unit that detected the incident will submit initial reports. The unit that detected the incident might not be the unit that caused the incident. The unit that caused the incident will direct additional reporting as warranted/required.

***b. (U) Amplifying Report***. This report will be submitted when there is new information regarding an incident for which an initial report has been submitted, or every 30 days until a final report is submitted. It may also serve as a final report.

***c. (U) Final Report.***

(1) (U) The final report will include a summary of the results of all inquiries and investigations, and it must identify corrective measures taken or planned to minimize the possibility of recurrence.

(2) (U) The final report may be incorporated with the initial report in those instances where all information concerning an incident has been obtained and there is no follow on information. (See Figure 7-2.)

***d. (U) Abbreviated Report.*** This report may be submitted during ground combat operations to report incidents involving the physical security of key. The report shall provide sufficient details to enable the CONAUTH to determine whether a compromise has, in fact, occurred. Therefore, the report must answer, at a minimum, the questions: *who, what, when, where, and how.* If the CONAUTH orders an unscheduled supersession of key as a result of the incident, a subsequent **complete** report must be submitted as soon as possible.

**7.3.3 (U) Report Precedence.**

**a. (U)** Initial and amplifying record reports of the following incidents will be assigned IMMEDIATE precedence; reports must be submitted as soon as possible, but no later than

**24 hours** after discovery of the incident or receipt of amplifying information.

(1) (U) Incidents involving currently effective keying material or keying material scheduled to become effective within 15 days.

(2) (U) Incidents involving defection, espionage, hostile cognizant agent activity, clandestine exploitation, enemy capture, tampering, penetration, sabotage, unauthorized copying, reproduction or photography.

(3) (U) When known compromise of RECENTLY (within 30 days) superseded key is detected, the incident will be reported immediately to all ACTION addressees and will be assigned IMMEDIATE precedence.

**b. (U)** Initial reports of the following incidents will be assigned PRIORITY precedence; the reports must be submitted as soon as possible, but not later than **48 hours** after discovery of the incident and upon receipt of amplifying information.

(1) (U) Incidents involving future keying material scheduled to become effective in more than 15 days.

(2) (U) Incidents involving superseded, reserve or contingency keying material.

(3) (U) Cryptographic incidents. Reports will be issued within **72 hours** from the time the incident was discovered.

**c. (U)** When preparing reports of Personnel Incidents and Physical Incidents involving COMSEC equipment (including that lost in satellites and space vehicles) and supporting documentation, assign a ROUTINE precedence to all addressees. Submit these reports as soon as possible, but no later than **72 hours** after discovery and upon receipt of additional information. You may assign higher precedence to reports that have potentially significant impact to national security.

**d. (U) Other Reportable COMSEC Incidents.** Initial and amplifying reports of any COMSEC Incident not covered in the preceding paragraphs, normally will be assigned ROUTINE precedence and must be submitted as soon as possible, but no later than 72 hours after discovery of the incident or upon receipt of amplifying information. However, originators should assign higher precedence to a report that has potential for significant impact.

## 7.4 ROUTING OF INCIDENT REPORTS.

**a. (U)** Incident reports are OFFICIAL command correspondence and will ALWAYS be submitted by or for the commander. All reports will be classified depending on their content; however, **all Personnel Incident Reports will be classified CONFIDENTIAL**. As a minimum, all other incident reports will be marked "FOR OFFICIAL USE ONLY" or classified, as appropriate. Reports will be addressed as shown in Table 7-2.

**b. (U)** In accordance with AR 380-40, paragraph 7-9c. (2)(d), COMSEC Incidents involving loss or theft of mission/Inter-theater COMSEC Package (ICP) key; falsification of records that result in a compromise of key; or any incident that may impact mission-critical Command, Control, and Communications (C3) operations will immediately be reported to HQDA, DCS, G-2 DAMI-CD by the Army CIMA.

**7.4.1 (U) Incident reports that involve Joint-Staff Position Control Material (Two-Person Control) and devices must be addressed IAW Joint Publication 1-04.**

**7.4.2 (U) Satellites and Space Vehicles.** When preparing reports pertaining to classified COMSEC equipment lost aboard satellites or other space vehicles that fail to reach or maintain orbit, the COMSEC material may be presumed destroyed upon reentry into the Earth's atmosphere. These losses will be reported as prescribed in Table 7-1 and paragraph 7.6.11.

Table 7-2. Incident Reporting Addressees

| TYPE OF INCIDENT | ACTION ADDRESSEE | INFO ADDRESSEE |
|---|---|---|
| Physical | 1. CONAUTH<br>2. DIRUSACCSLA, FT HUACHUCA AZ //SELCL-SAS-IN//<br><br>DMS Address: /C=US/O=U.S. Government/OU=DoD/OU= ARMY/OU=Organizations/L= CONUS/L=FORT HUACHUCA AZ/OU= CSLA/OU=CSLA Incidentdesk 1(uc) | 1. DIRNSA FT GEORGE G MEADE MD //I413// (See Note below.)<br>2. DIRUSACCSLA, FT HUACHUCA AZ //SELCL-ID-KEY//<br><br>DMS Address: /C=US/O=U.S. Government/ OU=DoD/OU=ARMY/OU=Organizations/ L=CONUS/L=FORT HUACHUCA AZ/ OU= CSLA/OU=CSLA ID Key<br><br>3. Local US Army Counterintelligence Support Unit<br>4. Appropriate Command Channels<br>5. Appropriate MACOM ISSPM<br>6. CSLA CIR if OCONUS |
| Key in distribution channels | 1. DIRNSA FT GEORGE G MEADE MD //I413//<br>2. DIRUSACCSLA, FT HUACHUCA AZ //SELCL-SAS-IN//<br>(See DMS address above.) | 1. CONAUTH<br>2. DIRUSACCSLA, FT HUACHUCA AZ // SELCL-ID-KEY//<br><br>DMS Address: /C=US/O=U.S. Government/ OU=DoD/OU=ARMY/OU=Organizations/ L=CONUS/L=FORT HUACHUCA AZ/ OU= CSLA/OU=CSLA ID Key<br><br>3. Local US Army Counterintelligence Support Unit<br>4. Appropriate Command Channels<br>5. Appropriate MACOM ISSPM |
| Key incident at CONAUTH level | DIRUSACCSLA, FT HUACHUCA AZ //SELCL-SAS-IN//<br>(See DMS address above.) | 1. DIRNSA FT GEORGE G MEADE MD //I413//<br>2. Local US Army Counterintelligence Support Unit<br>3. Appropriate Command Channels<br>4. Appropriate MACOM ISSPM |
| Equipment and Document | 1. DIRNSA FT GEORGE G MEADE MD //I413// (See Note below.)<br>2. DIRUSACCSLA, FT HUACHUCA AZ //SELCL-SAS-IN//<br>(See DMS address above.) | 1. DIRUSACCSLA, FT HUACHUCA AZ // SELCL-ID-KEY//<br><br>DMS Address: /C=US/O=U.S. Government/ OU=DoD/OU=ARMY/OU=Organizations/ L=CONUS/L=FORT HUACHUCA AZ/ OU= CSLA/OU=CSLA ID Key<br><br>2. Local US Army Counterintelligence Support Unit<br>3. Appropriate Command Channels<br>4. Appropriate MACOM ISSPM |
| Cryptographic | 1. DIRNSA FT GEORGE G MEADE MD //I413// (See Note below.)<br>2. DIRUSACCSLA, FT HUACHUCA AZ //SELCL-SAS-IN//<br>(See DMS address above.) | 1. Local US Army Counterintelligence Support Unit<br>2. Appropriate Command Channels<br>3. Appropriate MACOM ISSPM<br>4. CSLA CIR if OCONUS |

| Table 7-2. Incident Reporting Addressees (Continued) | | |
|---|---|---|
| Personnel | 1. DIRNSA FT GEORGE G MEADE MD //I413// (See Note below.)<br>2. DIRUSACCSLA, FT HUACHUCA AZ //SELCL-SAS-IN//<br>(See DMS address above.) | 1. Local US Army Counterintelligence Support Unit<br>2. Appropriate Command Channels<br>3. Appropriate MACOM ISSPM<br>4. CSLA CIR if OCONUS<br>5. CONAUTH (When Keying material is suspected to be involved.) |
| Administrative | Determined by the MACOM | CONAUTH |
| **Incident reports pertaining to STU-III will also be addressed to the NSA, ATTN: Y18** | | |

**7.4.3 (U) Discovery of Listening Devices.** Reporting instructions for the discovery of technical intercept devices (i.e., wiretaps or "BUGS") are covered in AR 381-14(S). Classification will be SECRET, as a minimum.

**7.4.4 (U) Compromising Emanations.** Loss of COMSEC information through compromising emanations will be reported to the Army Certified TEMPEST Technical Authority (CTTA). Telephone: Commercial (301) 677-4440.

## 7.5 TRANSMISSION DURING MINIMIZE AND "IN-THE-CLEAR."

**a. (U) Transmission During MINIMIZE.** Initial and Amplifying COMSEC Incident Reports are authorized for electrical transmission during periods of MINIMIZE, in accordance with AR 25-10. Final Reports; however, will NOT be electrically transmitted during MINIMIZE.

**b. (U) Transmission "In-the-Clear."**

**(1)** ***(U) Cryptographic Incidents.*** Reports of cryptographic incidents WILL NOT be transmitted in the clear.

**(2)** ***(U) Physical and Personnel Incidents.*** During tactical operations when the reporting command or activity may not have immediate access to secure electrical transmission, Initial and Amplifying Reports of COMSEC physical and personnel incidents may be transmitted in-the-clear, provided the commander has determined that immediate transmission is essential. Final Reports SHALL NOT be transmitted in the clear.

## 7.6 PHYSICAL INCIDENTS.

(U) The information contained in the following paragraphs is considered essential and must be included in incident reports.

**7.6.1 (U) Physical Incident Reports.** Include the following information in all Physical Incident Reports:

**a. (U) Account Identification.** COMSEC account number(s) and the unit(s) involved.

**b. (U) Material Identification.** Complete identification of the material involved in the incident, including:

(1) (U) Short Title (including edition designator).

(2) (U) Accounting/Serial Number(s) of ALC 1 and 6 (report other material by quantity).

(3) (U) Specific segments, tables, days, or pages involved (if not the complete document).

**c. (U) Keyed or Un-keyed.** If equipment or components were involved, indicate whether they were keyed or un-keyed.

**d. (U) Incident Description.** Provide a description of the incident, including the date and time of discovery, and answers to the questions: Who? What? When? Where? Why? How?

**e. (U) Compromise.** Estimate the probability of compromise (e.g., compromise is CERTAIN, PROBABLE, IMPROBABLE, POSSIBLE, or IMPOSSIBLE).

**f. (U) Key.** If key is involved, identify the CONAUTH(s).

**7.6.2 (U) Missing Material.** If the material involved is missing, also include the following:

**a. (U) Time and Place.** Report the date, location and circumstance of the last known sighting.

**b. (U) Cause of Loss.** Provide all available information pertaining to the cause of loss.

**c. (U) Actions Taken.** Describe all actions being taken to locate the material.

**d. (U) Unauthorized Access.** Indicate the possibility of access by unauthorized persons.

**e. (U) Disposal Method Used.** Explain the disposal method used for classified and unclassified waste.

**7.6.3 (U) Temporary Loss.** If the material is temporarily lost or otherwise out of proper channels, also include the following:

**a. (U) Time and Circumstances.** Indicate the exact period of time and under what circumstances the material was discovered to be out of proper channels.

**b. (U) Action**. Indicate the action that caused the material to be returned to proper channels.

**c. (U) Clearance Status.** Indicate the clearance status of persons having unauthorized access.

**d. (U) Surreptitious Access.** Indicate the possibility of surreptitious access by unauthorized persons.

**7.6.4 (U) Damaged Package.** If a package is damaged or shows evidence of possible tampering, also include the following:

**a. (U) Damage Description.** Provide a description of the damage and the extent to which the material could have been viewed. Take photographs from various angles and retain on file in case further investigation is required.

**b. (U) Transportation Method Used.** Indicate the method of transportation used (DCS, official courier, registered mail, etc.).

**c. (U) Circumstances.** Describe the circumstances that may have caused the damage or permitted possible unauthorized access to classified COMSEC material. If the information cannot be determined by local inquiry or investigation, the ACTION addressee will take action to have the shipment traced and all necessary information obtained. Once the information is available, another report will be submitted to supplement the Initial Report.

**d. (U) Unauthorized Viewing Contents.** If there was a possibility that unauthorized persons viewed the classified contents of a damaged package, report the Security Clearance status and nationality of each of those persons

**e. (U) Counterintelligence.** Indicate the identity of the counterintelligence (CI) unit that provided assistance during the investigation, if applicable.

**7.6.5 (U) Unauthorized Access**

(U) If it is known that unauthorized persons had access to classified COMSEC material or information (for even a very short time), your report will include the following:

**a. (U)** Indicate the identity of each person and their clearance status.

**b. (U)** Indicate the length of time the person(s) had access.

**c. (U)** Any COMSEC material to which the person had access.

**7.6.6 (U) Material Left Unprotected.**

**a. (U)** Unprotected material includes safes, containers, rooms or vaults that had been left open or unlocked or were discovered to have malfunctioning locking devices.

**b. (U)** In cases where the classified COMSEC material was left UNATTENDED or was not securely stored, the report will include the following:

(1) (U) Indicate the date and time period that the material was left unsecured.

(2) (U) Indicate the date and time the incident was discovered.

(3) (U) Explain when, by whom, and what actions were taken to secure the container or area.

(4) (U) Describe what security measures were in effect at the time the incident was discovered (i.e., guards, building kept locked, restricted area).

(5) (U) *Undetected Entry.* Indicate the possibility of an undetected entry into the area by unauthorized persons.

**7.6.7 (U) Aircraft Crashes.** Aircraft crashes will be reported as follows:

**a. (U) Crashed on Land.** If an aircraft should crash on land under combat, or non-combat conditions the report will include:

(1) (U) Location of crash (specify if in enemy-controlled territory).

(2) (U) Whether the crash area was secured, when, and by whom.

(3) (U) Whether the aircraft was completely destroyed by impact or explosion.

(4) (U) Whether or not the aircraft burned.

(5) (U) Whether or not the crash area was searched.

**b. (U) Crashed at Sea.** If the aircraft crashed at sea, the report will include:

(1) (U) Location of the crash. Give geographical coordinates, if available, or if close to shore, give approximate distances.

(2) (U) Approximate depth of water.

(3) (U) Whether or not material was in weighted containers.

(4) (U) Whether or not aircraft sank immediately.

(5) (U) Whether or not foreign vessels were in the immediate area.

**7.6.8 (U) Combat Conditions.** Under combat conditions, no further reports resulting from situations described in 7.6.7 and 7.6.8 are required unless recovery or salvage efforts are made, in which case the results of that effort should be reported. In addition, Final Reports are not required for material possibly compromised under ground combat conditions. Actions taken to recover COMSEC equipment missing due to actual combat operations should be comparable to actions taken to recover any other equipment assigned to the unit involved.

**7.6.9 (U) Unauthorized Photography.** Photographing CLASSIFIED COMSEC material is prohibited. This does not apply to its photocopy reproduction or microfilming for the purpose of producing an OFFICIAL record under proper controls and accountability, or to the photographing of an external view of a CCI equipment. Photographing CLASSIFIED COMSEC equipment requires specific written authorization from HQDA (DAMI-CD). (See AR 380-40.)

**7.6.10 (U) Satellites.** When classified COMSEC material is lost aboard a satellite or other space vehicle, report the equipment by short title and accounting number and give the launch time and the probable impact point on the earth's surface.

**7.6.11 (U) Controlled Cryptographic Items (CCI).**

**a. (U)** CCI are unclassified controlled end items or assemblies that perform a critical COMSEC or COMSEC ancillary function; however, when CCI contains key, it will be protected in a manner consistent with the classification of the information it processes.

Incident reports will be prepared accordingly. A security clearance is not required for access to CCI, but access shall be restricted to U.S. citizens whose duties require such access. Access may also be granted to permanently admitted, resident aliens who are U.S. Government civilian employees, active duty, or reserve members of the U.S. Armed Forces and whose duties require access.

**b. (U)** COMSEC Incidents involving un-keyed CCI (i.e., physical loss of CCI, tampering, theft) will be reported IAW DA PAM 25-380-2 and paragraph 7-2 of this TB.

## 7.7 PERSONNEL INCIDENTS.

**7.7.1 (U) Definitions.** The definition of a reportable personnel incident is as follows:

**a. (U)** When a person having access to classified COMSEC information is suspected of ESPIONAGE, DEFECTION, SUBVERSION, SABOTAGE, etc. (refer to Table 7-1).

**Or,**

**b. (U)** When a person who has been designated by the commander as having detailed knowledge of COMSEC equipment or manual cryptosystems is declared AWOL, is captured or presumed captured by enemy forces, becomes deceased under suspicious circumstances, or has had his or her security clearance revoked.

**c. (U)** DETAILED KNOWLEDGE is defined as an understanding of the crypto-principles of classified COMSEC equipment and CCI. This implies knowledge and understanding beyond that which even an efficient operator would require or possess.

**7.7.2 (U) Personnel Incident Reports.**

**a. (U)** As a minimum, all Personnel Incident Reports will be classified CONFIDENTIAL and contain the following information:

(1) (U) COMSEC Account Number.

(2) (U) The individual's full name, rank or grade, and SSN.

(3) (U) Date and circumstances of the incident.

(4) (U) Results of inventories and preliminary local investigations.

(5) (U) Results of CI interviews, interrogations and investigations.

(6) (U) List of missing COMSEC material or lists of all classified COMSEC material to which the person had access at the time of the incident. When the amount of material makes a message listing impractical, the list may be forwarded separately by the fastest available method.

(7) (U) A general statement of the individual's background in COMSEC and the extent of his/her knowledge of crypto-principles.

**b. (U) Final Reports.** Final Reports are required for Personnel Incidents. However, initial or subsequent reports may serve as the Final Report by adding a statement as follows: "The inquiry/interview/interrogation showed no evidence of possible compromise of classified COMSEC information. This is a Final Report."

**c. (U) Appropriate Action.** Appropriate action on individual incidents will be taken as specified in the following paragraphs.

**7.7.3 (U) Captured or Presumed Captured Personnel.** Within five days from the date the individual is returned to U.S. control or is declared dead, the commander will notify the NSA, Counterintelligence (CI) and CSLA.

**7.7.4 (U) Personnel Absence.** A report to the NSA is required if the commander makes a determination that an individual is absent or deceased under the criteria of paragraph 7.7.1.

**a. (U) Inventory of Classified COMSEC Material.** When any individual is declared absent per paragraph 7.7.1, an inventory of all classified COMSEC material to which the person had access will be made immediately. Also, a preliminary check will be made to determine the possibility of defection, subversion, or other crime.

**b. (U) CI Interview.** When an AWOL, DEFECTOR, or SUBVERSIVE is returned to U.S. control, CI personnel will interview the individual.

**7.7.5 (U) Revocation or Suspension of Clearance for Cause.**

**a. (U) Inventory of Classified COMSEC Material**. With the revocation or suspension of clearance for cause (e.g., serious violation of law or regulations which justifies revocation), an inventory of all classified COMSEC material to which the individual had access will be conducted immediately.

**b. (U) Defection or Subversive Intent.** A preliminary local check will be made to determine if there is any evidence to indicate the possibility of DEFECTION or SUBVERSIVE intent.

**c. (U) Compromise**. The individual will be interviewed and, if necessary, further inquiry made to determine if there has been any compromise of classified COMSEC information.

## 7.8 CRYPTOGRAPHIC INCIDENTS.

(U) Cryptographic incidents associated with each cryptosystem are identified in the operating (KAO) and maintenance (KAM) instructions. The following guide will be used in reporting Cryptographic Incidents:

**7.8.1 (U) Equipment Malfunctions.**

**a. (U)** Identify the equipment or components involved.

**b**. **(U)** Describe how, and under what conditions, the equipment was being used at the time of the incident.

**c. (U)** Identify the symptoms of the malfunction. Indicate, if applicable, the possibility that the malfunction was deliberately caused.

**d. (U)** If the equipment was used to send operational traffic, identify the TRAFFIC and the SHORT TITLE of any key involved.

**7.8.2 (U) Unauthorized Cryptoperiod Extension.** Should the incident involve an unauthorized EXTENSION of a prescribed cryptoperiod:

**a. (U)** Provide a detailed description of the associated communications activity (i.e., on-line/off-line, simplex/half duplex, transmit only/receive only, point-to-point/netted operation).

**b. (U)** Report the number of messages sent or received, and the general type of traffic involved.

## 7.9 ADMINISTRATIVE INCIDENTS.

**a. (U)** COMSEC Administrative Incidents are both administrative *and* COMSEC in nature in that they are insecure practices dangerous to security and they jeopardize the integrity of COMSEC material. Because of this danger, it is essential that positive action be taken by commanders to prevent their recurrence. These incidents, however, will be reported **only** within the Army chain-of-command as directed by the MACOM (at a minimum, the incident must be reported to the CONAUTH). Such reports will be retained on file for two years for review by Command Inspectors and Auditors.

**b. (U) The loss of a KOV-14 "User" Card is an Administrative Incident.** User cards are those KOV-14 cryptographic cards already assigned to a user and associated with a particular Secure Terminal Equipment (STE). When a user card is lost, users must promptly inform the COMSEC Custodian who will advise the chain-of-command of the loss, as well as report the incident to the COR and ask for Relief from Accountability because the KOV-14 Card is tracked in the CMCS. The COR will then remove the item from the account's assets and notify the NSA.

**(U//FOUO) EXCEPTIONS:** The following incidents involving the KOV-14 Card **must** be reported within 24-hours of discovery as COMSEC Incidents IAW paragraph 7.3 of this TB. Refer to NSTISSI 3030 for further information.

(1) (U) The loss of the user card occurs **with** its associated carry card.

(2) (U) The loss of a user card occurs **with** its associated STE.

(3) (U//FOUO) The lost card **was *not*** a user card, but a **fill** card.

(4) (U//FOUO) There is known or suspected tampering of the KOV-14 card.

(5) (U) There is a mismatch of keying material on the card and key tag (keying information can be verified after STE association).

**c. (U)** Reports of defective keying material and production errors are **not** considered reportable COMSEC Administrative Incidents. Such deficiencies are routine in nature and are reported directly to the NSA for resolution as an administrative matter.

## 7.10 INVESTIGATIONS.

**a.** (U) Normally, informal inquiries about reportable COMSEC Incidents will uncover sufficient information to determine whether or not a COMPROMISE has occurred and the measures recommended for preventing recurrence.

**b.** (U) Formal investigations may be required to determine certain violations of law or regulations. Such investigations will be conducted either at the discretion of the commander, as directed by cognizant authority, or as mandated by regulation. If there is an investigation, it will be conducted IAW AR 15-6. Investigating personnel will be properly cleared.

## 7.11 EVALUATIONS.

**a. (U)** The evaluation of information contained in an incident report is based not only on the information, but also on the security characteristics of the cryptosystem. Evaluations of incident reports must determine possible effects of the incident occurrence. The evaluation will routinely consist of CIMA personnel contacting the involved parties to determine if there were factors that led to compromise or loss of control of the material in question. As the responsible activity, CIMA (and/or the NSA) may direct further investigation or reporting in order ensure that a proper evaluation can be performed.

**b. (U)** When evaluation of the incident indicates that supersession of any item is necessary, the CONAUTH must immediately notify all holders of that item.

**c. (U)** When a cryptosystem has been declared compromised, it will NOT be used for further encryption unless it is operationally essential that encrypted messages are sent before the supersession date and an alternate system is not available. See also AR 380-40, paragraphs 7-9 and 7-10.

## 7.12 INCIDENT CASE FILES.

(U) Each COMSEC account must maintain case files for Reportable COMSEC Incidents. As a minimum, every case file will include:

**a. The Initial/Final Report(s)** as well as any Amplifying Reports, as needed. The Initial Report, or an Amplifying Report, could serve as the Final Report (see report descriptions in paragraph 7.1 of this TB).

**b. The CIMA Case Assignment Message.** If this message is not received within 30 days, the custodian must follow-up with the CIMA to ensure the incident report(s) were received and to ask for the status of the case.

**c. The COMSEC Incident Evaluation** issued by the appropriate agency (e.g., CIMA, NSA, CONAUTH).

**d. The Case Closure Message** issued by CIMA.

*(U) CCIRs will **not** be cleared if the account has pending incidents against it.*

## 7.13 REVIEWING AND MARKING COMPROMISED MESSAGES.

**7.13.1 (U) Reviewing Messages.** When classified operational key is considered compromised by the CONAUTH, the information encrypted with that key is also considered compromised. In this case, immediate action will be taken to review the national security information that has been compromised. The CONAUTH will also evaluate the resultant impact of such compromise on past, current and future operations. In some cases, corrective action can be taken to reduce or counteract the damage

caused by the compromise. Traffic reviews, that is, reviewing the record copy of messages encrypted in a compromised system, will be directed by the CONAUTH.

**7.13.2 (U) Marking Messages.** Messages involved in a compromise will not be automatically downgraded or declassified as a result of the compromise. Instead, the classified information contained in the message will be reevaluated, with downgrading or declassification being considered as directed by AR 380-5.

## 7.14 RELIEF FROM ACCOUNTABILITY.

**7.14.1 (U) Relief from CMCS Accountability.** Relief from CMCS accountability is granted by the Army COMSEC Incident Monitoring Activity (CIMA). The CIMA will provide a closure message to the COMSEC account and to the COR. The COR will, in turn, remove the material in question from the Army assets.

**7.14.2 (U) Relief from Property Accountability.**

**a. (U)** Relief from CMCS accountability will not be construed as relief from property accountability. In all cases of relief from CMCS COMSEC accountability, the following statement will be prepared, signed by the commander, and filed in the custodian's records: "The circumstances surrounding the loss of (identify material) have been considered and a determination has been made that a request for relief from property accountability (is/is not) required."

**b. (U)** It should be noted that relief from COMSEC accountability does not mean relief from responsibility for the loss, damage, or destruction of government property (see paragraph 2.9d of this TB).

***CONFIDENTIAL***
01 02 201438Z MAR 03 RR RR CCCC AA ZYUW TCC-1
NO
REPORTING ORGANIZATION
SEE TABLE 7-1
INFO: SEE TABLE 7-1
C O N F I D E N T I A L (CLASSIFICATION IS BASED UPON CONTENT)
SUBJECT: INITIAL/FINAL COMSEC INCIDENT REPORT (U)
A. (U) AR 380-40, CHAPTER 7, DTD XXXX
B. (U) TB 380-41, CHAPTER 7, DTD XXXX
1. (U) COMSEC ACCOUNT OF THE UNIT INVOLVED.
2. (C) MATERIAL IDENTIFICATION, COMPLETE ID OF THE MATERIAL, INCLUDING:
A. SHORT TITLE (INCLUDE EDITION DESIGNATOR)
B. ACCOUNTING/SERIAL NUMBER(S) OF ALC 1, 3, 6 AND 7 MATERIAL (OTHER MATERIAL BY QUANTITY).
C. SPECIFIC SEGMENTS, TABLES, DAYS, OR PAGES INVOLVED (IF NOT THE COMPLETE DOCUMENT).
3. (U) KEYED OR UN-KEYED. ONLY IF EQUIPMENT OR COMPONENTS WERE INVOLVED.
4. (C) INCIDENT DESCRIPTION, PROVIDE A DESCRIPTION OF THE INCIDENT, INCLUDE THE DATE AND TIME OF DISCOVERY, AND ANSWERS TO THE QUESTIONS WHO, WHAT, WHEN, WHERE, WHY AND HOW?
5. (C) COMPROMISE. ESTIMATE THE PROBABILITY OF COMPROMISE (E.G., COMPROMISE, NO COMPROMISE, OR COMPROMISE CANNOT BE RULED OUT).
6. (U) KEY. IF KEY IS INVOLVED, IDENTIFY THE CONAUTH(S).
7. (C) MISSING MATERIAL. IF THE MATERIAL INVOLVED IS MISSING, ALSO INCLUDE THE FOLLOWING:
A. DATE, LOCATION, ETC. LIST THE DATE, LOCATION AND CIRCUMSTANCE OF THE LAST KNOWN SIGHTING.
B. CAUSE OF LOSS. LIST ALL AVAILABLE INFORMATION PERTAINING TO THE CAUSE OF LOSS.
C. ACTIONS TAKEN. LIST ALL ACTIONS BEING TAKEN TO LOCATE THE MATERIAL.
D. UNAUTHORIZED ACCESS. INDICATE THE POSSIBILITY OF ACCESS BY UNAUTHORIZED PERSONS.
E. DISPOSAL METHOD USED. INDICATE THE DISPOSAL METHOD USED FOR CLASSIFIED AND UNCLASSIFIED WASTE.
8. (U) TEMPORARY LOSS. IF THE MATERIAL IS TEMPORARILY LOST OR OTHERWISE OUT OF PROPER CHANNELS, ALSO INCLUDE THE FOLLOWING:
A. TIME AND CIRCUMSTANCES. INDICATE THE EXACT PERIOD OF TIME AND UNDER WHAT CIRCUMSTANCES THE MATERIAL WAS DISCOVERED OUT OF PROPER CHANNELS.
B. ACTION. INDICATE THE ACTION THAT CAUSED THE MATERIAL TO BE RETURNED TO PROPER CHANNELS.
C. CLEARANCE STATUS. INDICATE THE CLEARANCE STATUS OF PERSONS HAVING UNAUTHORIZED ACCESS.
D. SURREPTITIOUS ACCESS. INDICATE THE POSSIBILITY OF SURREPTITIOUS ACCESS BY UNAUTHORIZED PERSONS.
9. (U) FOR ALL FINAL COMSEC INCIDENT REPORTS, INCLUDE CORRECTIVE ACTIONS IMPLEMENTED TO PREVENT A RECURRANCE OF THIS INCIDENT.
10. (U) POC. GIVE NAME, DSN, COMPLETE COMMERCIAL TELEPHONE NUMBER, FAX NUMBER, AND E-MAIL ADDRESS.

G. HENDERSON
124 INF DIV, 5932

DON OWEN, MAJ, CDR

DERIVED FROM: TB 380-41
DECLASSIFY ON: SOURCE MARKED OADR
DATE OF SOURCE: xxxx

***CONFIDENTIAL*** 201438ZMAR03

**Figure 7-1. Unclassified Example - Physical COMSEC Incident Report**

***CONFIDENTIAL***
01 02 201438Z MAR 03 RR RR CCCC AA ZYUW TCC-1
NO
REPORTING ORGANIZATION
SEE TABLE 7-1
INFO: SEE TABLE 7-1
C O N F I D E N T I A L (CLASSIFICATION IS BASED ON CONTENT)
SUBJECT: INITIAL/FINAL COMSEC INCIDENT REPORT (U)
A. (U) AR 380-40, CHAPTER 7, DTD XXXX
B. (U) TB 380-41, PARAGRAPH 5.24 THROUGH 5.33, DTD XXXX
1. (U) COMSEC ACCOUNT OF THE UNIT INVOLVED.
2. (C) THE INDIVIDUAL'S FULL NAME, RANK OR GRADE AND SSN.
3. (C) DATE AND CIRCUMSTANCES OF THE INCIDENT
4. (U) RESULTS OF INVENTORIES AND PRELIMINARY LOCAL INVESTIGATIONS.
5. (C) RESULTS OF CI INTERVIEWS, INTERROGATIONS AND INVESTIGATIONS.
6. (C) LIST OF MISSING COMSEC MATERIAL OR LISTS OF ALL CLASSIFIED COMSEC MATERIAL TO WHICH THE PERSON HAD ACCESS AT THE TIME OF THE INCIDENT. WHEN THE AMOUNT OF MATERIAL MAKES A MESSAGE LISTING IMPRACTICAL, THE LIST MAY BE FORWARDED SEPARATELY BY THE FASTEST AVAILABLE METHOD.
7. (C) A GENERAL STATEMENT OF THE INDIVIDUAL'S BACKGROUND IN COMSEC AND THE EXTENT OF HIS/HER KNOWLEDGE OF CRYPTO PRINCIPLES.
8. (U) FINAL REPORTS. FINAL REPORTS ARE REQUIRED FOR PERSONNEL INCIDENTS. HOWEVER, INITIAL OR SUBSEQUENT REPORTS MAY SERVE AS THE FINAL REPORT BY ADDING A STATEMENT AS FOLLOWS: "THE INQUIRY/INTERVIEW/INTERROGATION SHOWED NO EVIDENCE OF POSSIBLE COMPROMISE OF CLASSIFIED COMSEC INFORMATION. THIS IS A FINAL REPORT."
9. (U) POC. GIVE NAME, DSN, COMPLETE COMMERCIAL TELEPHONE NUMBER, FAX NUMBER, AND E-MAIL ADDRESS.

G. HENDERSON
124 INF DIV, 5932

DERIVED FROM: TB 380-41
DECLASSIFY ON: SOURCE MARKED OADR
DATE OF SOURCE: xxxx

DON OWEN, MAJ, CDR

***CONFIDENTIAL*** 201438ZMAR03

**Figure 7-2. Unclassified Example - Personnel COMSEC Incident Report**

***CONFIDENTIAL***
01 02 201438Z MAR 03 RR RR CCCC AA ZYUW TCC-1
NO
REPORTING ORGANIZATION
SEE TABLE 7-1
INFO: SEE TABLE 7-1
C O N F I D E N T I A L (CLASSIFICATION IS BASED ON CONTENT)
SUBJECT: INITIAL/FINAL COMSEC INCIDENT REPORT (U)
A. (U) AR 380-40, CHAPTER 7, DTD XXXX
B. (U) TB 380-41, PARAGRAPH 5.24 THROUGH 5.33, DTD XXXX
C. (U) DA PAM 25-380-2
D, (U) UNIT SUPPLY UPDATE
1. (U) DODAAC OF THE UNIT INVOLVED.
2. (C) MATERIAL IDENTIFICATION. COMPLETE IDENTIFICATION OF THE MATERIAL INVOLVED IN THE INCIDENT, INCLUDING: NOMENCLATURE, SERIAL NUMBER, AND QUANTITY. INDICATE WHETHER EQUIPMENT WAS KEYED OR UNKEYED.
3. (C) INCIDENT DESCRIPTION. PROVIDE A DESCRIPTION OF THE INCIDENT, INCLUDING THE DATE AND TIME OF DISCOVERY, AND ANSWERS THE QUESTIONS WHO, WHAT, WHEN, WHERE, WHY.
4. (U) COMPROMISE. ESTIMATE THE PROBABILITY OF POSSIBLE COMPROMISE, I.E., COMPROMISED, COMPROMISE CANNOT BE RULED OUT, OR NO COMPROMISE.
5. (U) KEY. IF KEY IS INVOLVED, IDENTIFY THE CONAUTH(S).
6. (U) MISSING CCI. IF THE MATERIAL INVOLVED IS MISSING, ALSO INCLUDE THE FOLLOWING: (THE LOSS OF CCI REQUIRES AN AR 15-6 INVESTIGATION IAW AR 735-5, PARAGRAPH 13-2A(6)).
A. DATE, LOCATION, ETC. LIST THE DATE, LOCATION AND CIRCUMSTANCES OF THE LAST KNOWN SIGHTING.
B. CAUSE OF LOSS. LIST ALL AVAILABLE INFORMATION PERTAINING TO THE CAUSE OF THE LOSS.
C. ACTIONS TAKEN. LIST ALL ACTIONS BEING TAKEN TO LOCATE THE MATERIAL.
D. POSSIBLE TAMPERING. INDICATE THE POSSIBILITY OF ACCESS BY UNAUTHORIZED PERSONS.
7. (U) TEMPORARY LOSS. IF THE MATERIAL IS TEMPORARILY LOST OR OTHERWISE OUT OF PROPER CHANNELS ALSO INCLUDE THE FOLLOWING:
A. TIME AND CIRCUMSTANCES. INDICATE THE EXACT PERIOD OF TIME AND UNDER WHAT CIRCUMSTANCES THE MATERIAL WAS DISCOVERED TO BE OUT OF PROPER CHANNELS.
B. ACTION. INDICATE THE ACTION WHICH CAUSED THE MATERIAL TO BE RETURNED TO PROPER CHANNELS.
C. CLEARANCE STATUS. INDICATE THE CLEARANCE STATUS OF PERSONS HAVING UNAUTHORIZED ACCESS.
D. SURREPTITIOUS ACCESS. INDICATE THE POSSIBILITY OF SURREPTITIOUS ACCESS BY UNAUTHORIZED PERSONS.
8. (U) INCLUDE CORRECTIVE ACTIONS IMPLEMENTED TO PREVENT A RECURRENCE OF THIS INCIDENT.
9. (U) POC. GIVE NAME, DSN, COMPLETE COMMERCIAL TELEPHONE NUMBER, FAX NUMBER, AND E-MAIL ADDRESS.

G. HENDERSON
124 INF DIV, 5932

DON OWEN, MAJ, CDR

DERIVED FROM: TB 380-41
DECLASSIFY ON: SOURCE MARKED OADR
DATE OF SOURCE: xxxx

***CONFIDENTIAL*** 201438ZMAR03

**Figure 7-3. Unclassified Example - CCI Incident Report**

**THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY**

# APPENDIX A

# REFERENCE REGULATIONS AND FORMS

**JOINT CHIEF OF STAFF PUBLICATIONS (CJCSI)**

| | |
|---|---|
| CJCSI 3260.01 (S) | Policy and Procedures Governing the Authentication and Safeguarding of Nuclear Control Orders (S) (replaced Joint Pub 1-04 [S]) |

**DEPARTMENT OF DEFENSE**

| | |
|---|---|
| DoD 5200.1-PH | DoD Guide to Marking Classified Documents |

**ARMY REGULATIONS (AR)**

| | |
|---|---|
| AR 15-6 | Procedures for Investigating Officers and Boards of Officers |
| AR 25-10 | Reduction and Control of Information Transfer in an Emergency |
| AR 25-11 | Record Communications and the privacy Communications System |
| AR 25-12 | Communications Security Equipment Maintenance and Maintenance Training |
| AR 25-55 | The Department of the Army Freedom of Information Act Program |
| AR 25-400-2 | The Modern Army Record keeping System |
| AR 66-5 | Armed Forces Courier Service (OPNAVST 5130.2; AFR 182.25) |
| AR 190-11 | Physical Security of Arms, Ammunitions and Explosives |
| AR 190-13 | The Army Physical Security Program |
| AR 190-16 | Physical Security |
| AR 310-49 | The Army Authorization Document System (TAADS) |
| AR 380-5 | Department of the Army Information Security Program |
| AR 380-40 | Policy for Safeguarding and Controlling Communications Security (COMSEC) Material |
| AR 380-67 | Department of the Army Personnel Security Program |
| AR 381-12 | Subversion and Espionage Directed Against the U.S. Army |
| AR 381-14 (C) | Technical Counterintelligence |
| AR 710-2 | Supply Policy Below the Wholesale Level |
| AR 710-3 | Asset and Transaction Reporting System |
| AR 725-50 | Requisition, Receipt, and Issue System |
| AR 735-5 | Policy and Procedures for Property Accountability |
| AR 735-11-2 | Reporting of the Item and Packaging Discrepancies |

**DEPARTMENT OF THE ARMY PAMPHLETS (DA PAM)**

| | |
|---|---|
| DA PAM 25-35 | Index of Communication Security (COMSEC) Publications |
| DA PAM 25-380-2 | Security Procedures of Controlled Cryptographic Items |
| DA PAM 710-2-1 | Using Unit Supply System (Manual Procedures)` |
| DA PAM 710-2-2 | Supply Support Activity Supply System: Manual Procedures |

**SUPPLY BULLETIN (SB)**

| | |
|---|---|
| SB 725-100-1 | Supply Support Activity Supply Systems: Manual Procedures |

**ARMY CRYPTOGRAPHIC OPERATIONAL GENERAL PUBLICATION (ARKAG)**

| | |
|---|---|
| ARKAG-1 (S) | Army COMSEC Publication, Status of COMSEC Key Material (U) |

**ARMY ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS) PUBLICATIONS**

| | |
|---|---|
| No Number Assigned | Army EKMS Workstation System Back-Up and Restore Procedures |
| No Number Assigned | LCMS Workstation Rebuild Procedures for SCO Unix Open server |
| EKMS 704B Vol 1 | LMD/KP Operator's Manual |
| EKMS 704B Vol 2 | LMD/KP Quick Steps and Troubleshooting Guide |

**NON-CRYPTOGRAPHIC OPERATIONAL GENERAL PUBLICATION (NAG)**

| | |
|---|---|
| NAG-16 | Field Generation of COMSEC Key/Tactical Operations |
| NAG-26 | Operational Security Doctrine/KYV-5, KY-99, KY-99A, KY-100 |
| NAG-47 | Operational Security Doctrine/AN/CYZ-10 |
| NAG-53 | Keying Standard for KG-84A/C and KIV-7 |
| NAG-69 | INFOSEC Policy and Procedures/FORTEZZA Card Certification Authority Workstation (CAW) |
| NAG-71 | Operational Security Doctrine LMD/KP |

**TECHNICAL BULLETINS (TB)**

| | |
|---|---|
| TB 11-7010-293-15-1 | Warranty Program for Army Key Management System (AKMS) AN/GYK-49(V) 1&2 |

**TECHNICAL MANUALS (TM)**

| | |
|---|---|
| TM 9-1300-206 | Ammunition and Explosives Standards |
| TM 11-7010-193-12 | Technical Manual Operator's and Unit Maintenance Manual, Computer Set, General |
| TM 43-0001-38 | Army Ammunition Data Sheets for Demolition Material |

**DEPARTMENT OF THE ARMY FORMS (DA)**

| | |
|---|---|
| DA FORM 1999-E | Restricted Area Visitor Register (Local Reproduction Authorized [LRA]) |
| DA FORM 2011-E | COMSEC Aids Items Register (Using Unit) |
| DA FORM 2011-1-E | COMSEC Equipment Items Register (Using Unit) |
| DA FORM 2028 | Recommended Changes to Publications and Blank Forms |
| DA FORM 2407 | Maintenance Request |
| DA FORM 2653-E | COMSEC Account - Daily Shift Inventory |
| DA FORM 3964 | Classified Document Accountability Record |
| DA FORM 4569 | Requisition Code Sheet |
| DA FORM 4669-E | COMSEC Material Voucher Control Register |
| DA FORM 5504 | Maintenance Request |
| DA FORM 5941-E | COMSEC Material Disposition Record |

**DEPARTMENT OF DEFENSE FORMS (DD)**

| | |
|---|---|
| DD FORM 1348 | DoD Single Line Item Requisition |
| DD FORM 2501 | Courier Authorization Card |
| DD FORM 254 | Department of Defense Contract Security Classification Specification Form |

**STANDARD FORMS (SF)**

| | |
|---|---|
| SF 153 | COMSEC Material Report |
| SF 700 | Security Container Information |
| SF 701 | Activity Security Checklist |
| SF 702 | Security Container Check Sheet |

**THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY**

# APPENDIX B

# ABBREVIATIONS AND TERMS

## B-1 ABBREVIATIONS

| | |
|---|---|
| ACCLAIMS | Army COMSEC Commodity Logistics, Accounting and Information Management System |
| ACCOR | Army COMSEC Central Office of Record, now referred to as the COR or Tier 1 at Fort Huachuca |
| ACES | Automated Communications Engineering Software |
| AKMS | Army Key Management System |
| ALC | Account Legend Code |
| ADP | Automatic Data Processing |
| AMC | US Army Material Command |
| AMDF | Army Master Data File |
| AR | Army Regulation |
| ARKAG | Army Cryptographic Operational General Publication |
| ARNG | Army National Guard |
| ASF | Army Stock Fund |
| AWCF | Army Working Capital Fund |
| BIOAPI | Biometric Application Program Interface |
| BPA | Blanket Purchase Agreement |
| C&C | Certification and Correction |
| C&E | Communications and Electronics |
| C4I | Command, Control, Communications, Computers and Intelligence |
| CAAD | COMSEC Army Address Directory |
| CARP | COMSEC Account Registration Packet |
| CCEP | Commercial COMSEC Endorsement Program |
| CCI | Controlled Cryptographic Item |
| CCIR | Change of Custodian Inventory Report |
| CCISP | Controlled Cryptographic Item Serialization Program |
| CCSS | Commodity Command Standard System |
| CECOM | Communications-Electronics Command |
| CEOI | Communication Electronics Operation Instructions |
| CER | Cryptonet Evaluation Report |
| CFA | COMSEC Facility Approval |
| CFAR | COMSEC Facility Approval Request |
| CI | Counterintelligence |
| CIIC | Controlled Item Inventory Code |
| CIK | Cryptographic Ignition Key |
| CIMA | COMSEC Incident Monitoring Activity |
| CIR | CSLA INFOSEC Representative |
| CLSC | COMSEC Logistics Support Center |
| CLSF | COMSEC Logistics Support Facility |
| CLSU | COMSEC Logistics Support Unit |
| CMCS | COMSEC Material Control System |
| CMDSA | COMSEC Material Direct Support Activity |
| CNCS | Cryptonet Control Station |
| CNSS | Committee for National Security Systems |
| COLA | Certificate of License and Authority |
| COMSEC | Communications Security |
| CONAUTH | Controlling Authority |
| CONUS | Continental United States |
| COOP | Continuity of Operations Plan |
| COR | Central Office of Record |
| COTS | Commercial Off the Shelf |
| CRYPTO | Cryptographic |
| CSA | COMSEC Servicing Account |
| CSLA | Communications Security Logistics Agency |
| CSS | Constant Surveillance Service |
| CT1S | Common Tier 1 System |
| CTTA | Certified TEMPEST Technical Authority |
| CUST | COMSEC Custodian |
| DA | Department of the Army |
| DACAP | DA Cryptographic Access Program |
| DAMPL | DA Master Priority List |
| DCS | Defense Courier Service |
| DESCOM | (US Army) Depot System Command |
| DIC | Document Identification Code |
| DIRNSA | Director, National Security Agency |
| DoD | Department of Defense |

| | |
|---|---|
| DODAAC | Department of Defense Activity Address Code |
| DODAAD | Department of Defense Activity Address Directory |
| DOIM | Director of Information Management |
| DRMO | Defense Reutilization Marketing Office |
| DTD | Data Transfer Device |
| EAC | Echelons Above Corps |
| EKMS | Electronic Key Management System |
| ERPSL | Essential Repair Parts Stockage List |
| ET1S | Extension Tier 1 Segment |
| F&AO | Finance and Accounting Office |
| FEDLOG | Federal Catalog |
| FOIA | Freedom of Information Act |
| FOUO | FOR OFFICIAL USE ONLY |
| FORSCOM | (US Army) Forces Command |
| G-2 | Assistant Chief of Staff (Intelligence) |
| G-4 | Assistant Chief of Staff (Logistics) |
| GSA | General Services Administration |
| HJ | Key Change (time) |
| HQDA | Headquarters Department of the Army |
| HR | Hand Receipt |
| HRH | Hand Receipt Holder |
| HSP | High Security Padlock |
| IAPM | Information Assurance Program Manager |
| IASO | Information Assurance Security Officer |
| IAW | In Accordance With |
| ICP | Inter-theater COMSEC Package |
| ID | Identification |
| IK | Installation Kit |
| INFOSEC | Information Security |
| INSCOM | Intelligence and Security Command |
| IOM | Installation/Operations/Maintenance |
| IP | Internet Protocol |
| IR | Items Register |
| ISS | Information Systems Security |
| ISSPM | Information Systems Security Program Manager |
| JCS | Joint Chiefs of Staff |
| J-SIIDS | Joint-Service Interior Intrusion Detection System |
| KAG | Cryptographic Operations General Publication |
| KAM | Cryptographic Operational Maintenance Manual |
| KAO | Cryptosystem Operating Instruction |
| KDC | Key Distribution Center |
| KEK | Key Encryption Key |
| KGC | Key Generation Center |
| KMI | Key Management Infrastructure |
| KP | Key Processor |
| LAA | Local Area Authorization |
| LCMS | Local COMSEC Management Software |
| LIN | Line Item Number |
| LMD | Local Management Device |
| LMM | Limited Maintenance Manuals |
| MACOM | Major Army Command |
| MARKS | Modern Army Record keeping System |
| MATCAT | Material Category |
| MCN | Management Control Number |
| MEVA | Mission Essential or Vulnerable Areas |
| MILDEPS | Military Departments |
| MILSTRIP | Military Standard Requisitioning and Issue Procedures |
| MOA | Memorandum of Agreement |
| MOU | Memorandum of Understanding |
| MOV | Material Obligation Validation |
| MRO | Material Release Order |
| MSC | Major Subordinate Command |
| MWO | Material Work Order |
| NAG | Non-Cryptographic Operational General Publication |
| NCS | Network Control Station |
| NEO | National Emergency Operations |
| NGB | National Guard Bureau |
| NICP | National Inventory Control Point |
| NLT | No Later Than |
| NLZ | No-Lone Zone |
| NMP | National Maintenance Point |
| NSA | National Security Agency |
| NSN | National Stock Number |
| NSTISSI | National Security Telecommunications and Information Systems Security Instructions |
| NTE | Not To Exceed |
| O&M | Operations and Maintenance |
| OCONUS | Outside Continental United States |
| OPCODE | Operational Code |
| OPM | Ordering Privilege Manager |
| OPSEC | Operational Security |
| OR | Office of Record |
| OTAR | Over the Air Re-key |
| OTC | One Time Code |
| OTD | One Time Disk |
| OTP | One Time Pad |
| OTT | One Time Tape |

| | |
|---|---|
| PAL | Permissive Action Link |
| PBO | Property Book Officer |
| PCB | Printed Circuit Boards |
| PCM | Positive Control Material |
| PCN | Product Control Number |
| PCS | Permanent Change of Station |
| PMHS | Physical Material Handling Segment |
| PSS | Protective Security Service |
| PT1S | Primary Tier 1 Segments |
| PTSN | Public Telephone System Network |
| RCS | Reports Control Symbol |
| RDD | Required Delivery Date |
| RDT&E | Research, Development, Testing and Evaluation |
| RICC | Reportable Item Control Code |
| ROTC | Army Reserve Officers' Training Corps |
| SAIR | Semiannual Inventory Report |
| SAS | Sealed Authority System |
| SBU | Sensitive But Unclassified |
| SC | Stockage Code |
| SCCC | Standardized COMSEC Custodian Course |
| SDNS | Security Data Network System |
| SF | Standard Form |
| SIGCEN | Signal Center |
| SIGINT | Signals Intelligence |
| SIGSEC | Signals Security |
| SIMS-X | Selected Item Management System- Expanded |
| SMA | Supply Management Army |
| SOI | Signal Operating Instruction |
| SOP | Standard Operating Procedures |
| SOS | Source of Supply |
| SRA | Specialized Repair Activity |
| SSA | Supply Support Activity |
| STANFINS | Standard Financial System |
| STARPUBS | Standard Army Publications System |
| TAADS | The Army Authorization Document System |
| TB | Technical Bulletin |
| TCMO | Theater COMSEC Management Office |
| TDA | Table of Distribution Allowances |
| TEK | Traffic Encryption Key |
| TM | Technical Manual |
| TOE | Table of Organizational Equipment |
| TPI | Two-Person Integrity |
| TS | Top Secret |
| TSCM | Technical Surveillance Countermeasures |
| TSEC | Telecommunications Security |
| TYAD | Tobyhanna Army Depot |
| UIC | Unit Identification Code |
| UCMJ | Uniform Code of Military Justice |
| USACCSLA | US Army CECOM, Communications Security Logistics Agency |
| USAR | US Army Reserve |
| USNDA | US National Distribution Authority |
| VDLS | Vaults, Depots, and Logistical System |
| VTAADS | Vertical-The Army Authorization Documents System |
| WWMCCS | Worldwide Military Command and Control System |

**B-2 TERMS**.

(U) Terms used in this TB and not contained in AR 310-25, or those having a different connotation from the AR 310-25 definition, are explained in the following paragraphs:

**(U) Access.** Access is the capability and opportunity to gain knowledge; or to alter information or material. (A person does not have access merely by being in a place where COMSEC material is kept, as long as security measures such as physical controls or authorized escorts deny opportunity to penetrate or exploit the material.)

**(U) Account Type Designator (ATD).** The ATD is the second position of the COMSEC account number, which identifies type of account (e.g., Theater COMSEC Management Office [TCMO], parent/COMSEC Material Direct Support Activities [CMDSA], administrative).

**(U) Accountability.** Accountability is the principle that an individual is responsible for safeguarding and controlling of COMSEC material entrusted to his/her care and is answerable to proper authority for the loss or misuse of that equipment or information. As a minimum, these records show debits, credits, and available on-hand or in-use balances. Records showing quantities due out and due in are part of the accountable records.

**(U) Accountable COMSEC Material.** All COMSEC keying material, COMSEC publications and classified COMSEC equipment and components are accountable COMSEC materials. Accountable COMSEC material is assigned an ALC and is controlled in the CMCS.

**(U) Accountable Officer.** The Accountable Officer is the person officially appointed, in writing, to maintain a formal set of accounting records of property or funds, whether public or quasi-public. This person may or may not have physical possession of the property or funds. Various types of Army Accountable Officers include:

a. **(U) COMSEC Custodian –** The COMSEC Custodian is the individual appointed, in writing, who is responsible for receipt, custody, security, accountability, safeguarding, inventory, transfer, and destruction of COMSEC material.

b. **(U) Alternate COMSEC Custodian.** The Alternate COMSEC Custodian is the individual responsible for the receipt, custody, security, accountability, safeguarding, inventory, transfer, and destruction of COMSEC material in the absence of the COMSEC Custodian.

c. **(U) Property Book Officer (PBO) –** The PBO is accountable for property on receipt until it is subsequently turned-in, used (consumed) for authorized purposes, or dropped from accountability. (Hand Receipt Holders are not considered Accountable Officers.)

d. **(U) Transportation Officer –** The Transportation Officer is accountable for property entrusted for shipment.

e. **(U) Stock Record Officer –** The Stock Record Officer is accountable for supplies being held for issue above the user level from time of receipt until issued, shipped, or dropped from accountability.

**(U) Accounting Legend Code (ALC).** The ALC is a numeric code used within the CMCS to indicate the minimum accounting controls required for COMSEC material.

**(U) Administrative Incident.** An Administrative Incident is an infraction of established COMSEC policies and procedures that is not as serious as the other COMSEC Incidents. An Administrative Incident is an insecure practice that requires reporting to the MACOM chain-of-command and the CONAUTH so that corrective action may be taken to ensure the violation does not recur. See paragraph 7.9 and Table 7-1, Section 4, of this TB for further information.

**(U) Advice code.** An Advice Code is used to transmit instructions considered by the initiator of requisitions to be essential to the desired supply action. Insertion of an advice code is at the discretion of the initial document requestor.

**(U) AKMS Document Number.** The AKMS Document Number is a 15-digit non-duplicative number constructed to identify the military service/requestor (COMSEC account number),

requisition date (using Julian Date) and 5-digit random computer generated serial number.

**(U) Army COMSEC Central Office of Record** (ACCOR). An obsolete term. See Central Office of Record (COR).

**(U) Army Key Management System (AKMS)** The Army's implementation of the EKMS. It provides real-time electronic key generation, distribution and management of existing COMSEC material. Provides compatibility and interoperability between all systems within DoD.

**(U) Army Master Data File (AMDF)**. The files required to record, maintain and distribute supply management data between Army commands and requiring activities.

**(U) Audit Trail – Audit Trail** documentation supports debit and credit entries on accounting records from the time property is brought into the inventory with a source document until the property is dropped from accountability.

**(U) Authorized Allowances of Equipment.** Equipment specified by an applicable Table of Allowances, Table of Organization and Equipment, Table of Distribution and Allowance, or Authorized Equipment Modification List.

**(U) Backorder.** That portion of requested stock not immediately available for issue and not passed to another source of supply for action is known as a backorder. A record of obligation to fill the backorder is known synonymously as a backorder or "due-out."

**(U) Backorder Release.** Stock issued on the basis of backorder records.

**(U) Card Privilege Authority (CPA).** The individual responsible for the configuration of user privileges and updates of the KOV-14 cryptographic card firmware. The CPA accesses the card's CPA privileges from any STE with a valid personal identification.

**(U) Central Facility (Tier 0).** A composite of the NSA's Ft. Meade and Finksburg key facilities that provide centralized key management services for all forms of key.

**(U) Central Office of Record (COR).** The Army activity charged with maintaining records of centrally accountable COMSEC material, monitoring accounting procedures and auditing COMSEC accounts within the Army.

**(U) Certificate of Verification.** Certification that a COMSEC account's Semiannual Inventory Report or the Change of COMSEC Custodian Report has been verified against the accounting records at the Central Office of Record.

**(U) Certification and Correction (C&C) Page.** A manually prepared last page of the pre-printed Semiannual Inventory Report or pre-printed Change of Custodian Report. The C&C page contains additions and deletions correcting the report and the certification of the custodian and witness attesting to the accuracy of the report.

**(U) Cognizant Security Authority.** That entity, staff element or individual within a department, agency, or subordinate command echelon designated to serve in such capacity, and charged with responsibility on behalf of a commander, Director, or civilian equivalent for the physical, technical, personnel, and information security management related to all matters affecting that command. Within Army commands, there is a hierarchy of **Cognizant Security Authorities,** which exist at MACOMs, major subordinate commands, intermediate command structures, geographical command areas, and installations, with each cognizant security authority having delegated sole jurisdiction within that command element for all security-related matters (e.g., J-2, G-2, S-2) and equivalent automation security authorities (e.g. DOIM, ISSO, ISSM). (See also the definition for Competent Authority.)

**(U) Common Fill Devices.** A family of devices developed to read in, transfer, and store key (e.g., the AN/CYZ-10 Data Transfer Device (DTD), the KYK-13 Electronic Transfer Device, the KOI-18 General Purpose Tape Reader, and the KYX-15A Net Control Device).

**(U) Communications Security (COMSEC).** Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC equipment.

**(U) Competent Authority.** As used in this publication in the control, physical protection and accounting for COMSEC material, a **Competent**

**Authority** is any person specifically designated and delegated the authority by a commander, or equivalent civilian personage (within the scope of his or her authority), to make determinations and decisions pertaining to COMSEC management. Such individuals must be in a recognized position of responsibility within an organization or activity, and must possess the requisite training, experience, technical knowledge, demonstrated trust, and professional qualities, which inspire the full confidence of the commander and subordinate elements.

**(U) Compromise.** A compromise is any known or presumed disclosure of classified data to unauthorized persons, 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. (See COMSEC Compromise.)

**(U) COMSEC Account Number**. A COMSEC Account Number is a six-character alphanumeric identifying each activity responsible for maintaining custody and control of accountable COMSEC material.

**(U) COMSEC Account Registration Packet (CARP).** Used to register or modify EKMS IDs.

**(U) COMSEC Accountability.** The obligation of an officially designated custodian of a COMSEC account to maintain formal records of accountable COMSEC material for the purpose of providing proper security, accounting and reporting.

**(U) COMSEC Accounting.** The established procedures for positive and continuous control of COMSEC material from time of receipt through destruction or final disposition.

**(U) (COMSEC) Administrative Incident.** See Administrative Incident.

**(U) COMSEC Compromise.** A COMSEC Compromise occurs when the COMSEC material is irretrievable or lost, or when available information clearly proves that the material was made available to an unauthorized person.

**(U) COMSEC Custodian.** The COMSEC Custodian is the individual appointed, in writing, who is responsible for receipt, custody, security, accountability, safeguarding, inventory, transfer, and destruction of COMSEC material. (See Accountable Officer.)

**(U) COMSEC Equipment.** COMSEC equipment is designed to provide security to telecommunications by converting information into an unintelligible form to an unauthorized interceptor and by reconverting such information to its intended form for authorized recipients, as well as equipment designed specially to aid in, or as an essential element of, the conversion process. COMSEC equipment is crypto-equipment, crypto-ancillary equipment, crypto--production equipment and authentication equipment.

**(U) COMSEC Equipment End Item.** These items are equipment or a combination of component parts ready for their intended use in a COMSEC application.

**(U) COMSEC Facility (CF).** A CF operates, maintains, researches, develops, tests, evaluates and/or stores COMSEC material.

**(U) COMSEC Facility Approval Request (CAR).** A CAR is used when a requirement exists to either establish or update the COMSEC Facility Approval. (See Figure 2-1.)

**(U) COMSEC Incident, Reportable.** See Reportable COMSEC Incident.

**(U) COMSEC Incident Monitoring Activity.** This is the office within a department or agency that maintains a record of COMSEC Incidents caused by elements of that department or agency. The Activity ensures that all actions required of those monitored elements are completed.

**(U) COMSEC Insecurity.** A COMSEC Insecurity is any incident that has been investigated, evaluated, and determined to jeopardize the security of COMSEC material or the secure transmission of information.

**(U) COMSEC Key and Publications.** A generic term for COMSEC material, other than equipment or devices, that assists in securing telecommunications and which is required in the production, operation, or maintenance of COMSEC systems and their components (e.g., COMSEC keying material, call sign/frequency systems and supporting documents such as operating and maintenance manuals).

**(U) COMSEC Key.** A COMSEC key is a sequence of random, binary bits used to initially set-up and to periodically change permutations in crypto-equipment for purposes of encrypting or decrypting electronic signals.

**a. (U) Traffic Encryption Key (TEK).** A key used to encrypt plain text or to super-encrypt previously encrypted text and/or decrypts cipher text.

**b. (U) Key Encryption Key (KEK).** A key that encrypts and/or decrypts other keys for transmission (re-keying) or storage.

**c. (U) Transmission Security Key (TSK).** A key that is used to control transmission security processes (e.g., frequency hopping and spread spectrum).

**d. (U) Key Production Key (KPK).** A KPK is key that is used to initialize a key-stream generator for the production of other electronically generated keys.

**(U) COMSEC Logistics.** The Army system for acquisition, storage, movement, distribution, security, accounting, maintenance and disposition of COMSEC material. (This supplements AR 310-25.)

**(U) COMSEC Logistics Support Center (CLSC).** The facility providing COMSEC logistics support to a field Army or equivalent force and other activities, as directed.

**(U) COMSEC Logistics Support Facility (CLSF).** An organization assigned a primary mission of COMSEC logistics support. CLSFs include TCMO, CLSC, and CLSU.

**(U) COMSEC Logistics Support Unit (CLSU).** The facility providing COMSEC logistics support to a Corps or on a geographical area basis.

**(U) COMSEC Material.** Items designed to secure or authenticate communications. COMSEC material includes, but is not limited to: key, equipment (including CCI), devices, documents, firmware or software that embodies or describes cryptographic logic, and other items that perform COMSEC functions.

**(U) COMSEC Material Control System (CMCS).** The logistics system through which accountable COMSEC material is distributed, controlled and safeguarded. It consists of COMSEC Central Offices of Record (COR), depots and COMSEC accounts.

**(U) COMSEC Publications.** For the purposes of this TB, COMSEC publications are defined as documents and manuals that are produced at the NSA, assigned an ALC number, accountable in the CMCS, and are requisitioned within the Army from USACCSLA (SELCL-ID-KEY). All other Army documents pertaining to COMSEC policy and procedures and equipment operation and maintenance are requisitioned through the Standard Army Publications Systems (STARPUBS) using the DA 12-series Forms (e.g., Army equipment TMs, DA Pam 25-35, and this TB).

**(U) COMSEC Reportable Material.** Accountable COMSEC material requiring periodic inventory and reconciliation with Tier 1 to ensure stringent accounting and centralized control within the Army is COMSEC Reportable Material.

**(U) COMSEC Retail Level.** The COMSEC Retail Level is the level of logistics support below the COMSEC Wholesale level. COMSEC Logistics Support Facilities and COMSEC Material direct Support Activities are units that are engaged in retail level supply support.

**(U) COMSEC Wholesale Level.** The COMSEC Wholesale Level is the COMSEC supply and maintenance support, which includes USACCSLA and Tobyhanna Army Depot. The wholesale system procures supplies for the Army from commercial sources or government plants. COMSEC wholesale supply support is accomplished by distributing COMSEC material to retail levels for stockage or for issue to users.

**(U) Contingency Keying Material.** Key designed for, distributed to, and held by a command to satisfy specific operational requirements or in support of specific contingency plans.

**(U) Controlled Cryptographic Item (CCI).** An unclassified controlled secure telecommunications or automated information handling equipment and associated cryptographic assembly, component, or other hardware item that performs a critical COMSEC or COMSEC ancillary function. Items so designated will bear the designation “Controlled Cryptographic Item” or “CCI.”

**(U) Controlling Authority (CONAUTH).** The commander of the organization or activity responsible for directing the establishment and operation of a Cryptonet and for managing the operational use and control of keying material assigned to the Cryptonet.

**(U) CRYPTO.** A marking or designator identifying all COMSEC key used to protect or authenticate telecommunications carrying classified national security information and sensitive, unclassified Government or Government-derived information: the loss of which could adversely affect national security interests. CRYPTO keying material is controlled in the CMCS.

**(U) Crypto-ancillary Equipment.**

**a. (U)** Equipment designed specifically to facilitate efficient or reliable operation of crypto-equipment, but which does not perform cryptographic functions.

**b. (U)** Equipment designed specifically to convert information to a form suitable for processing by crypto-equipment.

**(U) CRYPTO compromise.** The compromise of CRYPTO information or recovery of plain text of an encrypted message by unauthorized persons through crypto-analysis.

**(U) Crypto-equipment.** Any equipment that embodies a cryptographic logic is known as crypto-equipment.

**(U) Cryptographic Logic.** The well-defined procedure, sequence of rules or steps used to encrypt/decrypt plain text information or to produce a key stream; plus the delays, alarms, and checks which are essential to effective performance of the cryptographic process.

**(U) Cryptographic Ignition Key (CIK).** A device or variable used to unlock the secure mode of crypto-equipment. A CIK can split or alter the crypto-variable so that keyed crypto-equipment may be left unattended without being zeroized when the CIK is removed.

**(U) Cryptographic Incidents.** A Cryptographic Incident is defined as any equipment malfunction, operator, or COMSEC manager/custodian error that adversely affects the cryptosecurity of a machine, auto-manual or manual cryptosystem.

**(U) Cryptonet Control Station.** The communications terminal responsible for generating, distributing and/or managing key variables is the Cryptonet Control Station.

**(U) Design Controlled Repair Part.** A part, subassembly or assembly for any COMSEC equipment or device with an NSA-controlled design that has been sent for repair. Used primarily in NSA design-controlled cryptologic equipment systems and assigned the Commercial and Government Entity (CAGE) code 98230. These items are procurable only as directed by the NSA. *Fabrication or procurement of these items will not be made without approval and authorization by the NSA*.

**(U) Document Identifier Code (DIC).** A three-digit MILSTRIP/MILSTAMP code which identifies the basic type of administrative action, the specific sub-type of supply transaction and related modifying instructions for each type of supply document and movement document. The Document Identifier Code is used throughout the requisitioning, processing, and issuing functions, or in other types of supply transactions within and between supply distribution systems.

**(U) Document Number.** A 14-digit, non-duplicative number constructed to identify the military service/requestor (COMSEC Account number), requisition date (using Julian Date) and serial number.

**(U) Document Register.** A record of document numbers assigned to supply documents. It serves as a suspense file for open supply transactions. They are kept by calendar or fiscal year. Units operating COMSEC accounts will have a separate document register for classified COMSEC items managed and will be controlled by the COMSEC Custodian.

**(U) Edition.** An Edition is any number of like copies of a specific cryptosystem or authentication system. Editions are identified by letters or numbers after the item designation in the short title.

**(U) Electronic Key.** A generic team used to encompass all locally-, Tier 1- or Central Facility- generated keying material, FIREFLY and modern key and imported key.

**(U) Electronic Key Management System (EKMS).** A system developed to automate the CMCS to improve the speed and efficiency of key management and to provide new capabilities for generating and managing electronic key. EKMS is not a separate key management system but can be used to track the CMCS material in all its forms. This system will enable COMSEC Custodians to generate most of their own key by use of a Key Processor. EKMS will be used by all DoD services and the Civil Agencies.

**(U) Embedded Cryptography.** Cryptography that is installed into an equipment or system whose basic function is not cryptographic is embedded. Components comprising the cryptographic module are inside the equipment or system and share host device power and housing. The cryptographic function may be dispersed or identifiable as a separate module within the host.

**(U) Explicit Key.** ALC 6/7 key that is provided automatic control by EKMS in accordance with distribution restrictions prescribed by the controlling authority.

**(U) HJ Time.** HJ Time is an established time period used to change from one edition or segment to another edition or segment, as so determined by the controlling station.

**(U) Implicit Key.** ALC 6/7 key whose handling characteristics are determined solely by policy and procedural means are Implicit Key.

**(U) Key Generation Facilities.**

**a. (U) Fixed key generation facility.** A COMSEC Facility that is located in an immobile structure or aboard a ship and in which COMSEC key in electronic form is generated.

**b. (U) Transportable key generation facility.** A transportable field facility in which the electronic form of COMSEC key is generated (e.g., a KG-83 TRI-TAC key variable generator van).

**c. (U) Mobile key generation facility.** A mobile field facility that can be readily moved from one location to another and which generates COMSEC key in electronic form (e.g., a tactical net control station equipped with VINSON crypto-equipment and a KYX-15A net control device). The Key Processor (KP) is a cryptographic component in EKMS designed to provide for the local generation of keying material, the encryption and decryption of key, key loading into fill devices, and to provide message signature functions.

**(U) Key Steam.** A sequence of symbols (or their electrical or mechanical equivalents) produced in a machine or auto-manual cryptosystem. These symbols combine with plain text to produce cipher text, to control the TRANSEC process, or to produce other keys.

**(U) Limited Maintenance Manual (LMM).** LMMs are requisitioned through STARPUBS. They are NSA-produced maintenance manuals on CCI equipment. They differ from NSA KAMs in that they are not controlled within the CMCS and are not assigned an ALC.

**(U) Local Element.** A “local element” (Hand Receipt Holder) is a new term used in EKMS. LCMS provides the option (by the custodian) to hand receipt material to a “local element.” The entry in LCMS could be a serial number from a fill device, an individual’s name, or a unit name

**(U) Local Management Device (LMD).** A component in EKMS that provides automated services for the management of key and other COMSEC material and an interface to the Key Processor.

**(U) Local COMSEC Management Software (LCMS).** Software which resides on the LMD and performs EKMS functions such as accounting, auditing, distribution, ordering, production, system administration, operator interface services, and platform-dependent services. Provides the capabilities to manage and account for electronic key, physical key, and other COMSEC material such as equipment and manuals.

**(U) Machine Cryptosystem.** This is a cryptosystem in which the cryptographic processes are performed by crypto-equipment.

**(U) Manual Cryptosystem.** This is a cryptosystem in which the cryptographic processes are performed manually without the use of crypto-equipment, limited protection equipment, or auto-manual devices.

**(U) No-Lone Zone.** An area, room, or space which, when manned, must be occupied by two or more appropriately cleared individuals who remain within sight of each other is known as a No-Lone Zone.

**(U) Non-accountable COMSEC Material.** COMSEC material not requiring formal accountability in the CMCS is considered non-accountable COMSEC material. This material consists of all unclassified COMSEC equipment. Unclassified COMSEC equipment is assigned a CIIC of "9" (CCI) or "U" (unclassified) in the AMDF. See also: Accountable COMSEC Material.

**(U) On-Line Crypto-operation.** This is use of crypto-equipment that is directly connected to a signal line; thus making encryption and transmission, reception and decryption, or both together, a single continuous process.

**(U) Personnel Incidents.** A Personnel Incident is any capture, attempted recruitment, unauthorized disclosure of COMSEC information, attempts by unauthorized persons to effect such disclosure, known or suspected control by a hostile intelligence entity, or unauthorized absence or defection of an individual having knowledge of or access to COMSEC information or material.

**(U) Physical incidents.** A Physical Incident is defined as the loss; theft; loss of control; capture; recovery by salvage; tampering; or the unauthorized viewing, access or photography of any classified COMSEC material, Controlled Cryptographic Item (CCI), or unclassified key marked "CRYPTO."

**(U) Physical (COMSEC) Material.** COMSEC is a generic phrase used to encompass all "Hard Copy" key, software, publications, equipment items and hardware.

**(U) Positive Control Material.** Material which requires continuous surveillance and control at all times by a minimum of two authorized individuals: each capable of detecting incorrect and unauthorized procedures with respect to the task being performed, and each being familiar with established security and safety requirements IAW JCS Pub 1-04 (S) is Positive Control Material. (Formerly known as Two-person Control Material.)

**(U) Report of Survey.** The Report of Survey is an instrument for recording circumstances concerning the loss, damage, or destruction of Army property. Serves as, or supports, a voucher for dropping articles from property records on which they are listed. Also serves to determine the question of responsibility (pecuniary or otherwise) for the absence or condition of the articles. (Not used for CMCS Accounting. See paragraph 5.)

**(U) Reportable COMSEC Incident.** A Reportable COMSEC Incident is any occurrence that potentially jeopardizes the security of COMSEC material or the secure electrical transmission of national security information or of information governed by 10 USC, Section 2315. These incidents are to be reported to the NSA and the Tier 1 IAW Chapter 7 of this TB. (See Table 7-1, Sections 1 – 3 for a listing of these types of incidents.)

**(U) Reserve Keying Material.** This is key which is not designated for a specific command, but which is held by a CLSF, or may be distributed to and held by a given command, in anticipation of a possible requirement to establish a new unplanned or unforeseen Cryptonet on short notice.

**(U) Service Authority**. The Service Authority is the command or activity within each military service that oversees Communications Security (COMSEC) operations, policy, procedures and training. Service Authority responsibilities are those functions that the military services have determined cannot be performed by the CT1. Service Authority roles include cryptographic hardware management and distribution control, including Foreign Military Sales (FMS); approving account establishments; approving authority for Certification Approval Authorities (CAAs); implementing COMSEC Material Control System (CMCS)/Key Management Infrastructure (KMI) policy and procedures; direct operational support; final adjudication authority for determining when reported COMSEC Incidents result in COMSEC insecurities; ensuring service compliance with COMSEC access program requirements; and standing membership on KMI working groups and the CT1 Joint Configuration Control Board (JCCB).

**(U) Supply Bulletin.** Supply Bulletins are publications providing technical or non-technical information required to maintain support items.

**(U) Table of Distribution and Allowances (TDA).** TDA is a table that prescribes the organizational structure, personnel and equipment authorization and requirements of a military unit so they may perform a specific mission in which there is no appropriate Table of Organization and Equipment.

**(U) Table of Organization and Equipment (TOE).** TOE is a table that prescribes the normal mission, organizational structure, and personnel and equipment requirements for a military unit.

**(U) Technical Bulletin (TB).** A TB is a publication that contains technical information pertaining to weapons, equipment and professional techniques.

**(U) Technical Manual.** A manual providing detailed treatment of specific subjects considered necessary for the full accomplishment of required training. A technical manual also contains descriptions of material and instructions for operation, handling, maintenance and repair.

**(U) Telecommunications.** The preparation, transmission, communication, or processing of information, (writing, images, sounds or other data) by electrical, electromagnetic, electromechanical, or electro-optical means is called telecommunications.

**(U) Terminal Privilege Authority (TPA).** The TPA is the individual responsible for the configuration of the STE security features, the upgrade of the terminals software, and the inspection of the terminals physical integrity.

**(U) Test Equipment.** The electric, electronic, mechanical, hydraulic or pneumatic equipment that is either automatic, manual or any combination thereof, which is required to perform the checkout function.

**(U) Theater COMSEC Logistics Support Center (TCLSC).** The TCLSC Facility provides COMSEC logistics support to Army forces in a theater of operations and to other activities, as directed.

**(U) Tier 0.** See Central Facility.

**(U) Tier 1.** A layer of EKMS that serves as the intermediate key generation and distribution center, Central Office of Record (COR), privilege manager, and registration authority for EKMS Tier 2 accounts. Tier 1 maintains a continuous and exact record of centrally accountable (ALC 1, ALC 2, and ALC 6) COMSEC material located at Ft Huachuca, AZ, and Lackland Air Force Base, TX.

**(U) Tier 2.** A layer of EKMS comprised of the COMSEC accounts that manage key and other COMSEC material.

**(U) Tier 3.** The lowest layer of EKMS. This is the COMSEC material user/Hand Receipt Holder.

**(U) Traditional versus Manual.** This term is interchangeable throughout this TB and refers to non-automated (EKMS) accounts.

**(U) TSEC Nomenclature.** TSEC is a system for identifying the type and purpose of items classified COMSEC material over which the NSA exercises configuration control. TSEC is an abbreviation for telecommunications security.

**(U) Two-person Integrity (TPI).** TPI is a system of storage and handling designed to prohibit individual access to certain COMSEC keying material by requiring the presence of at least two authorized persons: each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed.

**(U) Unit Identification Code (UIC).** A UIC uniquely identifies each unit of the active Army, Army National Guard and the United States Army Reserve.

**(U) User Account.** A COMSEC account established to use COMSEC material.

**(U) Validation Authority.** The Army Global Positioning System (GPS) Validating Authority is responsible for verifying the operational necessity of GPS in an organization's mission and for ensuring users request the proper key material with the correct short title. The Validating Authority for the Army is CSLA.

**THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY**

# APPENDIX C

# COMSEC NOMENCLATURE SYSTEMS

## C-1 GENERAL

**(U)** The COMSEC nomenclature systems described in the following paragraphs are identification systems for NSA-produced or authorized U.S. COMSEC material.

## C-2 DEFINITIONS

**(U)** The following definitions apply to corresponding terms used in this TB:

**C-2.1 Advanced Development Model (ADM). (U)** ADM is the model of a completed piece of COMSEC equipment for experimentation or test to demonstrate the technical feasibility of the design. This equipment has the ability to meet existing performance requirements and to secure engineering data for further development.

**C-2.2 (U) Assembly.** A group of parts, elements, subassemblies, or circuits assembled as a separately removable item of COMSEC equipment.

**C-2.3 (U) COMSEC Equipment System.** A COMSEC Equipment System is a grouping of COMSEC equipment, which, of itself, provides communications security for a particular communications link, terminal, or switching center.

**C-2.4 (U) Element.** An element is a subdivision of an equipment, assembly, or subassembly that normally consists of a single item or a group of replaceable parts. It is a removable item necessary to the operation of equipment, but it does not necessarily perform a complete function in itself.

**C-2.5 (U) Engineering Development Model (EDM).** An EDM is a model to be used for engineering or operational tests under service conditions for evaluation of performance and military suitability.

**C-2.6 (U) Exploratory Development Model (XDM).** An XDM is an assembly of preliminary circuits and parts in line with commercial practices to investigate, test, or evaluate the soundness of a concept, device, circuit, equipment, or system in breadboard or rough experimental form without regard to the eventual overall design form.

**C-2.7 (U) Long Title.** A Long Title is a full, descriptive title assigned to an item of COMSEC material on the basis of the type and function of the particular item. Whenever feasible, long titles are worded to be UNCLASSIFIED and under no circumstances are terms included which reveal the type of cryptographic principle or features of logic.

**C-2.8 (U) Pre-production Model.** A pre-production model is suitable for complete evaluation. It is completely representative of the final equipment.

**C-2.9 (U) Production Model.** A production model is an equipment model in its completed mechanical and electrical production design.

**C-2.10 (U) Release Prefix.** A Release Prefix is a combination of letters to indicate the foreign release status of COMSEC keying material. “A” is assigned to material produced for the use by the U.S. and specified allies, wherein the U.S. control over the material exists or is implied, “U.S.” is assigned to material for exclusive U.S. use.

**C-2.11 (U) Short Title.** Short Titles are an identifying combination of letters and numbers assigned to COMSEC material for brevity (e.g., KAM-211A/TSEC, TSEC/KG-30).

**C-2.12 (U) Subassembly.** A subassembly is a major subdivision of an assembly that consists of a package of parts, elements, and circuits, which perform a specific function.

## C-3 MYTHOLOGICAL DESIGNATORS

**(U)** For general ease of reference, the names of ancient, mythological characters (e.g., DIANA, ORESTES, ROMULUS) are assigned to certain general cryptosystems used by the U.S. and its allies when a signal cryptosystem is embodied in several different forms. The decision to assign a mythological designator to a particular system rests with the Deputy Director of NSA for COMSEC, and his/her assignments become formal when they appear on the specifications for the associated COMSEC key. Mythological designators, the association of such designators, and tier-related meanings are UNCLASSIFIED.

## C-4 NSA COVER-NAMES

**(U)** During the early stages of the development cycle of NSA-developed COMSEC equipment, cover-names (e.g., PARKHILL, VINSON, BELLFIELD) were assigned for convenience in differentiating the various evolving programs. After TSEC nomenclature is assigned, and until the equipment goes into production, the NSA cover-name is normally shown in correspondence inside parentheses. Although these cover-names are officially dropped from correspondence when an equipment enters its first production contract, they sometimes continue in colloquial use as system designators.

## C-5 TSEC NOMENCLATURE (for Non-CCI Material)

**C-5.1 (U) Assignment.** TSEC nomenclature may be assigned to COMSEC equipment as soon as the decision to develop it for user evaluation has been made. Assembly, subassembly, and element designators are assigned upon identification of the equipment's internal configuration. TSEC nomenclature is assigned to all U.S.-produced COMSEC key and publications prior to their production. COMSEC-related documents, such as Communications Security Equipment Engineering Bulletins (CSEEBs), informational Technical Bulletins (TBs), and Communications Security Equipment Systems Documents (CSESDs) are not assigned TSEC nomenclatures. In addition, TSEC nomenclature is not assigned to interconnecting boards, extender boards, board extractors, mounting bases, interconnecting cables, repair and spare parts containers, carrying cases, control panels, and most adapter units—or to commercial items.

**C-5.2 (U) Amendments.** COMSEC short titles are not normally amended and specifically will not be amended to show changes in classifications, copy count, number of holders, relationship to another short title, mythological designator, intended usage, or modification status. The Director of NSA (DIRNSA) is responsible for procurement and distribution of nameplates required as a result of modification, re-designation, or reclassification of all U.S.-produced COMSEC equipment held by federal departments or agencies.

**C-5.3 (U) Equipment Short Titles.** The short title assigned to classified COMSEC equipment is comprised of the following elements, in order shown:

**a. (U)** The nomenclature system designator "TSEC" followed by a slant ("/").

**b. (U)** A function designator consisting of a descriptive digraph followed by a dash. Descriptive digraphs are selected from Table C-1 and consist of a general function designator to show the basic function, which the equipment performs, and a type designator to show the general type of the equipment. In correspondence and technical documentation (never on nameplates), a TSEC short title may be followed by an unfilled parenthesis, for example: TSEC/KG-30( ), to denote a series or line of equipment models.

**c. (U)** An item number.

**d. (U)** A model designator, when appropriate. The model designators "X" (exploratory development), "V" (advanced development), "E" (engineering development), and "P" (pre-production) are employed to designate COMSEC equipment at the various evolutionary stages in the development cycle. Model designators are not assigned to production models of COMSEC equipment.

**C-5.4 (U) Assembly Short Titles.** The short titles assigned to COMSEC assemblies are comprised of the following elements in the order shown:

**a. (U)** A descriptive tri-graph selected from table C-1 followed by a dash. Trigraphs indicate the function and type designators of the equipment of which the assembly is a part and the specific type of function performed by the assembly. Assembly numbers are assigned to correspond, whenever possible, to the number of the equipment with which the assembly is used. In circumstances wherein equipment contains more than one functionally similar assembly not interchangeable with another, each such assembly is distinguished by a dash plus number following the assembly (e.g., the HNT-10-1/TSEC is a 4-channel master transmitter for TSEC/HN-10 Data Multiplexing Ancillary Equipment, while the HNT-10-2/TSEC is a 4-channel supplemental transmitter and received for the same equipment).

**b. (U)** An item number.

**c. (U)** A model designator, when appropriate (see C-5.3d).

**d. (U)** The nomenclature system designator "TSEC" preceded by a slant ("/").

**C-5.5 (U) Subassembly Designators.** The system designator "TSEC" is not used in subassembly short titles. The designator assigned to COMSEC subassemblies is comprised of the following elements, in the order shown:

**a. (U)** The letter "Z" followed by a dash.

**b. (U)** A unique alphabet trigraph that begins with AAA and continues through ZZZ.

**C-5.6 (U) Element Designators.** The system designator "TSEC" is not used in element short titles. The designator assigned to COMSEC elements is comprised of the following, in the order shown:

**a. (U)** The letter "E" followed by a dash.

**b. (U)** A unique alphabetic trigraph, which begins with AAA and continues through ZZZ.

**C-5.7 (U) COMSEC Equipment System Designators.** System designators are used to identify a group of equipment, which function together. They may be used in correspondence or technical documentation, but do not appear on equipment nameplates. The short titles assigned to COMSEC equipment systems are comprised of the following elements, in the order shown:

**a. (U)** The nomenclature system designator "TSEC" followed by a slant ("/").

**b. (U)** A function-type designator consisting of a descriptive digraph followed by a dash. The descriptive digraph is selected from Table C-1 and includes the letter "C" as the function designator and a type designator to show the general type of the system. Variations of a basic COMSEC equipment system are identified by a suffix consisting of a dash and a number (e.g., CY-2-1 is the Narrowband Secure Voice System-Ground Terminal).

**c. (U)** An item number.

**C-5.8 (U) Modification Designators.**

**a. (U)** Each modification made to the production model of a COMSEC equipment or assembly which results in loss of interchangeability of component parts between the modified and unmodified versions (but not loss of cryptographic intercommunicability) is identified by the addition of a modification suffix letter to the short title of the modified equipment or assembly (e.g., TSEC/KG-30B).

**b. (U)** Each modification made to an equipment or assembly which affects neither cryptographic intercommunicability nor physical interchangeability is identified by an appropriate marking on the modification record plate affixed to the modified equipment or assembly, or by the appropriate modification number placed on the modified equipment or assembly. The short title of the modified equipment is unchanged.

**c. (U)** Repair actions made to an equipment or assembly are not identified by any markings but are fully documented by maintenance manual changes.

**d. (U)** Modification of subassemblies or elements that affect neither cryptographic intercommunicability nor physical interchangeability is identified by a modification number preceded by a slant (e.g., E-FNN/1).

**e. (U)** When subassemblies or elements are modified to the extent that either physical interchangeability or cryptographic intercommunicability is lost, a new trigraph is assigned to the modified subassembly or element.

**f. (U)** Change of equipment within a COMSEC equipment system does not necessarily change the system designator.

**C-6 TSEC SHORT TITLES FOR COMSEC KEY.**

**(U)** Similar nomenclature schemes are employed for designating key (including wired hardware items such as programmable read-only memory [PROMs], read-only memory [ROMs], and large-scale integrated circuits [LSIs]) and other documents, such as general, operating, and maintenance manuals.

**C-6.1 (U) TSEC Short Titles for Key.** Short titles assigned to COMSEC key (including key produced in the form of integrated circuit devices such as PROMs, ROMs, and LSIs) are comprised of the following elements, in the order shown:

**a. (U)** A release prefix, "US" or "A." Refer to Table C-2.

**b. (U)** The functional relationship, purpose and type aid designators selected from Table C-2.

**c. (U)** An item number preceded by one space character.

**d. (U)** An edition letter or number 1 preceded by one space character.

**e. (U)** Part designator, when appropriate.

**C-6.2 (U) TSEC Short Titles for COMSEC Publications.** Short titles for general, operating and maintenance documents are comprised of the following elements, in the order shown:

**a. (U)** Functional relationship, purpose and type key designators selected from Table C-2 (e.g., KAG, KAO, KAM).

**b. (U)** An item number preceded by a dash.

**c. (U)** An edition letter 1.

**d. (U)** The nomenclature system designation "TSEC" preceded by a slant ("/").

**C-7 SHORT TITLES FOR SPECIAL COMSEC KEY.**

**C-7.1 (U) Short Titles for NATO COMSEC Key.** Short titles for NATO COMSEC Key are comprised of the following elements, in the order shown:

**a. (U)** The nomenclature system designator "AMS" 2.

**b. (U)** The type aid designator.

| | | |
|---|---|---|
| (1) | (U) Authentication | A |
| (2) | (U) Code | C |
| (3) | (U) One-time pad | D |
| (4) | (U) General Publication | G |
| (5) | (U) Recognition/ Identification | I |
| (6) | (U) Key list | K |
| (7) | (U) Miscellaneous | L |
| (8) | (U) Maintenance manual | M |
| (9) | (U) Operating manual | O |
| (10) | (U) Rotor | R |
| (11) | (U) One-time tape | T |
| (12) | (U) Key card | Y |

**c. (U)** An item number preceded by a space character key.

**d. (U)** An edition letter.

**C-7.2 (U) Short Titles for AUS-NZ-CAN-UK-US KEY.** Short titles for COMSEC Keys used mutually between Australia, New Zealand, Canada, the United Kingdom, and the United States are comprised of the following elements, in the order shown:

**a. (U)** The nomenclature system designator "CC."

**b. (U)** The type aid designator selected from Table C-2.

**c. (U)** An item number preceded by a space character.

**d. (U)** An edition letter or number preceded by one space character.

(1) (U) Edition letters are assigned to general documents and to regularly superseded key beginning with “A” and proceeding sequentially through “ZZZ.” Edition designators for irregularly preceded key begin with “1” and ascend sequentially through “999999”.

(2) (U) Exercise and training editions are identified by the digraphs “TX” and “TC,” respectively, and are inserted immediately after “AMS”.

**Table C-1**

**Function and Type Designators for COMSEC Equipment, Equipment Systems and Assemblies**

**Equipment Function (1st Letter)**

| | | |
|---|---|---|
| C | _ | COMSEC Equipment System |
| K | _ | Cryptographic |
| H | _ | Crypto-ancillary |
| M | _ | Manufacturing |
| N | _ | Non-cryptographic |
| S | _ | Special Purpose |

**Equipment Type (2nd Letter)**

| | | |
|---|---|---|
| G | _ | Key Generation |
| I | _ | Data Transmission |
| L | _ | Literal |
| N | _ | Signal Conversion |
| O | _ | Multi-Purpose |
| P | _ | Material Production |
| S | _ | Special Purpose |
| T | _ | Testing and Checking |
| U | _ | Television |
| W | _ | Teletypewriter |
| X | _ | Facsimile |
| Y | _ | Speech |

**Assembly Type (3rd Letter)**

| | | |
|---|---|---|
| A | _ | Advancing |
| B | _ | Base or Cabinet |
| C | _ | Combining |
| D | _ | Drawer or Panel |
| E | _ | Strip or Chassis |
| F | _ | Frame or Rack |
| G | _ | Key Generator |
| H | _ | Keyboard |
| I | _ | Translator or Reader |
| J | _ | Speech Processing |
| K | _ | Keying |
| L | _ | Repeater |
| M | _ | Memory or Storage |
| O | _ | Observation |
| P | _ | Power Supply, Converter |
| R | _ | Receiver |
| S | _ | Synchronizing |
| T | _ | Transmitter |
| U | _ | Printer |
| V | _ | Removable COMSEC Component |
| W | _ | Logic Programmer Programming |
| X | _ | Special Purpose |

**Table C-2**

**Functional Relationship, Purpose and Type Designator**

**for COMSEC Key Material**

**Release Prefix (1st Letter)**

US -- Indicates item is not releasable to foreign nationals

A -- Indicates item is authorized for release to specified allies

**Functional Relationship (2nd Letter)**

C _ Two-man Control
K _ Cryptographic
H _ Ancillary
M _ Manufacturing
N _ Non-cryptographic
S _ Special Purpose

**Purpose (3rd Letter)**

A _ Operational
B _ Compatible Multiple Keying Variable
L _ Logistics Combinations
M _ Maintenance
R _ Reference
S _ Sample
T _ Training
V _ Developmental
X _ Exercise
Z _ "On-the-Air" Test/training

**Type Aid (4th Letter)**

A _ Authenticator
B _ Diagnostic Test Program
C _ Code/Cipher
D _ Obsolete
E _ Diskette
F _ Cryptographic Program
G _ General Publication
H _ Call Sign and /or Frequency Change System
I _ Recognition and/or Identification System
J _ Indicator List
K _ Key List
L _ Miscellaneous
M _ Maintenance Manual
N _ Computer Keying Material
O _ Operating Manual
P _ One-Time Pad
Q _ Engineering Document
R _ Rotor
S _ Sealed Authentication System
T _ Tape
U _ Prom/Rom/LSI Devices
V _ Communications-Electronics Operating Instructions (CEOI)
X _ Fanfold Pan
Y _ Key Card
Z _ Permuting Plug

**THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY**

# APPENDIX D

# REPRODUCIBLE FORMS

**D-1. (U) REPRODUCTION OF FORMS**

**(U)** The following electronic forms are authorized for local reproduction; however, the data elements on all forms, excluding item i (Sample, Electronic Key Management Worksheet, Figure D-8), MUST remain the same.

**a. (U) DA Form 1999-E, Restricted Area Visitor Register (Figure D-1).** Reproduce this form on 8½ x 11-inch white paper printed head to foot.

**b. (U) DA Form 2011-E, COMSEC Aids Items Register (Figure D-2).** Reproduce this form on 8½ x 11-inch white paper printed head to foot.

**c. (U) DA Form 2011-1-E, COMSEC Equipment Items Register (Figure D-3).** Reproduce this form on 8½ x 11-inch white paper printed head to foot.

**d. (U) DA From DA Form 2653-E, COMSEC Account Daily Shift Inventory (Figure D-4)**. Reproduce this form on 8½ x 11-inch white paper printed head to foot.

**e. (U) DA Form 4669-E, COMSEC Material Voucher Control Register (Figure D-5, Front).** Reproduce this form on 8½ x 11-inch white paper printed head to foot. Side 2 of 2 is to be printed on the reverse of side 1 of 2.

**f. (U) DA Form 4669-E, COMSEC Material Voucher Control Register (Figure D-5, Reverse).** Reproduce this form on 8½ x 11-inch white paper printed head to foot. Side 2 of 2 is to be printed on the reverse of side 1 of 2.

**g. (U) DA Form 5251-E, CONAUTH Key Management Worksheet (Figure D-6).** Reproduce this form on 8½ x 11-inch white paper printed head to foot.

**h. (U) DA Form 5941-E, COMSEC Material Disposition Record (Figure D-7).** Reproduce this form on 8½ x 11-inch white paper printed head to foot.

**i. (U) Sample, Electronic Key Management Systems Worksheet (Figure D-8).** (This is a sample worksheet; however, custodians may design a worksheet that will better fit their needs. As long as the pertinent information: Short Title, Edition, Segment #, All Signatures and Date of Destruction, is included.) Reproduce this form on 8½ x 13-inch white paper printed head to foot.

**D-2 (U) The DA Forms listed above are also available in electronic format on the Army Electronic Library (AEL) CD-ROM (EM0001) and on the USAPA website at www.usapa.army.mil.**

| RESTRICTED AREA VISITOR REGISTER<br>For use of this form, see TB-380-41; the proponent agency is AMC | | | | | | | ORGANIZATION | | YEAR | | | Requirements Control Symbol - AMC-226 (Ri) | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DATE | | | | | | | PURPOSE OF VISIT | CLEARANCE STATUS (TS,S, Conf, None) | MATERIAL STORED OR SCREENED | | AUTHORIZING OFFICER'S SIGNATURE | TIME | |
| DAY | MO | PRINTED NAME *(First MI, Last)* | GRADE | SSN | SIGNATURE | ORGANIZATION | | | YES | NO | | IN | OUT |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |

**DA *FORM 1999-E, JUL 03*** EDITION OF JAN 1988 IS OBSOLETE

**PRIVACY ACT STATEMENT**
**"Authority: 10 USC 3012/EO.**
**SSN is used only for identification.**
**Access to this COMSEC Facility may be denied without SSN."**

**Figure D-1. DA Form 1999-E, Restricted Area Visitor Register**

| **COMSEC AIDS ITEMS REGISTER** *(Using unit)* | For use of this form, see TB 380-41; the proponent agency is AMC | | | |
|---|---|---|---|---|
| SHORT TITLE | NSN/MCN | LOCATION | ALC | ACCOUNT NO |

| EDIT/ REG | SERIAL NUMBERS | | RECEIPT | | DISPOSITION | | DEST/ ISSUE DATE | DESTRUCTION CERTIFICATION |
|---|---|---|---|---|---|---|---|---|
| | BEGIN | END | FROM | DATE / SERIAL | TO | DATE / SERIAL | | 1. CUSTODIAN 2. WITNESS |
| | | | | | | | | 1. |
| | | | | | | | | 2. |
| | | | | | | | | 1. |
| | | | | | | | | 2. |
| | | | | | | | | 1. |
| | | | | | | | | 2. |
| | | | | | | | | 1. |
| | | | | | | | | 2. |
| | | | | | | | | 1. |
| | | | | | | | | 2. |
| | | | | | | | | 1. |
| | | | | | | | | 2. |
| | | | | | | | | 1. |
| | | | | | | | | 2. |
| | | | | | | | | 1. |
| | | | | | | | | 2. |
| | | | | | | | | 1. |
| | | | | | | | | 2. |
| | | | | | | | | 1. |
| | | | | | | | | 2. |

DA FORM 2011-E
1 JUL 03

THIS FORM, TOGETHER WITH DA FORM 2011-1-E, 1 JUL 03
REPLACES DA FORM 2011, 1 NOV 77, WHICH IS OBSOLETE.

| **COMSEC EQUIPMENT ITEMS REGISTER** *(Using unit)* | | | | | | | | | | | For use of this form, see TB 380-41; the proponent agency is AMC |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SHORT TITLE | | | | NSN/MCN | | | END ITEM | | | ALC | ACCOUNT NO |
| QTY | SERIAL NUMBERS | | RECEIPT | | | TRANSFER | | | LOAN DATA | | ON HAND BALANCE |
| | BEGIN | END | ACCOUNT | DATE | SERIAL NUMBER | ACCOUNT | DATE | SERIAL NUMBER | FROM | DURATION | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

DA FORM 2011-1-E
1 JUL 03

THIS FORM, TOGETHER WITH DA FORM 2011-E, 1 JUL 03
REPLACES DA FORM 2011-1, 1 NOV 77, WHICH IS OBSOLETE

**COMSEC ACCOUNT – DAILY SHIFT INVENTORY**

**For use of this form, see TB 380-41; the proponent agency is AMC**

WHEN FILLED IN, THIS FORM WILL BE CLASSIFIED IN ACCORDANCE WITH TB 380-41

| SHORT TITLE | QTY | REG. NO | SHIFT | DAY OF THE MONTH | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 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 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SHORT TITLE | QTY | REG. NO | DAY | 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 |
| MONTH | | SHIFT 1 | INITIALS | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| PAGE NUMBER | | SHIFT 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NUMBER OF PAGES | | SHIFT 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**DA** FORM JUL 03 **2653-E**

**Figure D-4. DA Form 2653-E, COMSEC Account Daily Shift Inventory**

## COMSEC MATERIAL VOUCHER CONTROL REGISTER

For use of this form, see TB 380-41; the proponent agency is AMC

| 1. ACCOUNT NUMBER | 2. DATES (Day, month, year) | |
|---|---|---|
| | a. FROM | b. TO |

| 3. ORGANIZATION/ACTIVITY | 4. UIC | 5. PAGE |
|---|---|---|
| | | |

| 6. VOUCHER NUMBER | 7. TO | 8. DCS REGISTERED NUMBER | 9. TYPE TRANSACTION | 10. REMARKS |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

DA Form 4669-E JUL 03

EDITION OF 1 NOV 77 IS OBSOLETE
**EDITION OF AUG 90 IS OBSOLETE**

**Figure D-5 (Front). DA Form 4669-E, COMSEC Material Voucher Control Register (Side 1 of 2)**

FOR OFFICIAL USE ONLY

| 6. VOUCHER NUMBER | 7. TO | 8. DCS REGISTERED NUMBER | 9. TYPE TRANSACTION | 10. REMARKS |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

*REVERSE OF DA FORM 4669-R, AUG 90*
***REVERSE OF DA FORM 4669-E JUL 03***

**Figure D-5 (Reverse). DA Form 4669-E, COMSEC Material Voucher Control Register (Side 2 of 2)**

FOR OFFICIAL USE ONLY

(CLASSIFIED WHEN FILLED IN)

**CONAUTH KEY MANAGEMENT WORKSHEET**

For use of this form, see TB 380-40; the proponent agency is INSCOM.

| CONAUTH | CNCS | DATE |
|---|---|---|
| | | |

| KEY ID *a* | KEY TYPE *b* | CLASS *c* | EQUIPMENT TYPE *d* | CRYPTO PERIOD *e* | EFFECTIVE DATE *f* | ALT CNCS *g* | SUBSCRIBER ID *h* | DISTRIBUTION POC *i* | REMARKS *j* |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

DA Form 5251-E JUL 03

EDITION OF MAR 86 IS OBSOLETE

(CLASSIFIED WHEN FILLED IN)

Figure D-6. DA Form 5251-E, CONAUTH Key Management Worksheet

FOR OFFICIAL USE ONLY

## COMSEC MATERIAL DISPOSITION RECORD

**For use of this form, see TB 380-41; the proponent agency is AMC**

| 1. SHORT TITLE | 2. REG/EDIT | 3. SEC CLASS | 4. SERIAL NUMBER | 5. EFFECTIVE DATE |
|---|---|---|---|---|
| | | | | |

| 6. NR OF KEYS | 7. NR OF COPIES | 8. TOTAL NR OF SEGMENTS | 9. CONTROLLING AUTH | 10. CRYPTO PERIOD |
|---|---|---|---|---|
| | | | | |

| 11. SEGMENT/DAY | 12. ISSUE TO/DATE USED | 13. DESTROYED BY/DEST DATE | 14. WITNESSED BY/DATE |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**DA FORM 5941-E JUL 03**

**Figure D-7. DA Form 5941-E, COMSEC Material Disposition Record**

## Electronic Key Management Worksheet

**Worksheet is Confidential when filled with operational data**

| Electronic Key Management (EKM) Worksheet | | | | | | | | GENERATING EKMS ID | | CONAUTH | | | | HR # | DATE |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Short Title | Edition | Segment # | Variable Type | Class. | A L C | Equipment Type | Cryptoperiod | Effective Date | Date of Issue | Authorized Recipient Signature | Destroy Date | Date of Destruction | Signature of Destruction Official | Signature of Destruction Witness | |
| | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |

1. * **Generating EKMS ID** — LMD COMSEC Account that generated this electronic key
2. **CONAUTH** — Controlling authority for this key.
3. **HR #** — Hand Receipt number from which material is distributed.
4. **Date** — Date the EKM worksheet is generated.
5. * **Short Title** — COMSEC material item designation, which identifies the material i.e., USED XXXX. Key Tag could also be entered in this block.
6. * **Edition** — The letters or numbers following the item designation in the short title i.e. USED XXXX Edition A.
7. * **Segment #** — The specific segment within the edition.
8. **Variable Type** — Key Encryption Key (KEK) and or Traffic Encryption Key (TEK).
9. **Class.** — Enter the security classification of the Short Title.
10. **Equipment Type** — List the COMSEC equipment for which the Short Title was generated (i.e. KG-84A, KIV-7 etc.).
11. * **Cryptoperiod** — State the cryptoperiod for the segment: 24hrs/1 day, 1 week, 1 month, etc.
12. * **Effective Date** — State the date segment is effective.
13. **Date of Issue** — Date segment was issued to authorized recipient.
14. * **Authorized Recipient Signature** — Signature: Authorized recipient.
15. * **Date of Destruction** — Enter date segment was destroyed.
16. * **Signature of Destruction Official** — Signature: Person performing segment destruction.
17. * **Signature of** Destruction Witness — Signature: Person witnessing the segment destruction.

NOTE : * **Information should be on all EKM Worksheets.**

**Figure D-8. Electronic Key Management System Worksheet**

**THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY**

# APPENDIX E

# COMSEC ACCOUNT REGISTRATION PACKET (CARP)

## PROCEDURES FOR COMPLETING THE COMSEC ACCOUNT REGISTRATION PACKET

**(U) Within the Army, the COMSEC Account Registration Packet has replaced the DA Form 2012. This replacement was necessary due to the implementation of the Army Key Management System (AKMS). The COMSEC Account Registration Packet contains items that are necessary for inclusion into a national central database that will be maintained by the Tier 1 system and the National Security Agency (NSA). All Army COMSEC accounts, whether traditional or Army Key Management System (AKMS), must complete this packet when submitting changes to their account structure. This packet will always be submitted to CSLA who, within the Electronic Key Management System, acts as the Registration Authority (RA) for the Army.**

1. (U) The following step-by-step instructions are provided to assist in the completion of the COMSEC Account Registration Packet. The packet and the instructions have been designed to incorporate the COMSEC Account Registration, as well as Electronic Key Management System (EKMS) registration. The information provided should be based on the operational capabilities of the account.

2. (U) Within the Army, all classified COMSEC equipment, physical key, electronic key and/or any other COMSEC Material Control System (CMCS) accountable material must be received and maintained in a properly established COMSEC account. In addition, those COMSEC Accounts receiving electronic key must register the EKMS attributes of the account with the Registration Authority (CSLA) and the Central Facility (the NSA). The COMSEC Account Registration Packet accomplishes this requirement.

3. (U) One EKMS ID number will be assigned per account. For Command Authorities (CA) and User Representatives (UR) not associated with a COMSEC account, the Tier 1 RA will assign an EKMS ID.

4. (U) The following information explains the various sections of the form, defines the data needed, and identifies if the data is required or optional. The RA is the only element in the EKMS hierarchy that can submit the registration packets to the NSA for Army COMSEC Accounts.

**<u>REGISTRATION PACKET DETAILED INSTRUCTIONS:</u> This format is designed for use by all Army Users.**

**(U) Servicing Tier 1 Registration Authority ID: <u>LEAVE BLANK.</u>** When Tier 1 is operational, the Army accounts will be divided between the Primary Tier 1 Site (PT1S) located at Fort Huachuca, AZ, and the PT1S located at San Antonio, TX. Until that transition is accomplished, your Servicing COR EKMS ID will be "5A6151." Each account will be notified, in advance, if their account has been randomly selected for transfer to the PT1S located at San Antonio, TX. At that time, the account will be provided with the new EKMS ID of their servicing COR.

**1. (U) Agency Submitting Request:** <u>LEAVE BLANK.</u> **For Tier 1 RA Use ONLY.**

**2. (U) Account Submitting Request:**

**Agency Name**: Enter your unit name (i.e., 346th Signal Battalion, Fort Gordon, GA).

**Affiliation:** "ARMY" will always be entered here. The required data has been provided for you on the account registration packet.

**Active Army/National Guard/Government Contractor/Reserves:** Check the appropriate response regarding the unit submitting the registration packet.

**3. (U) Type of Action:** (The unit must complete the entire registration packet regardless of the type of action annotated).

**a. (U) Register New Account:** Used when establishing new COMSEC accounts, EKMS account privileges at a COMSEC account or to assign an EKMS ID to an account. If you are a Command Authority (CA) or User Representative (UR), check this block. *CAs and URs must still be registered at the Central Facility at Finksburg as they are using the CA and UR Registration forms supplied by Finksburg. Your EKMS ID number will be your current COMSEC account number. Provide the 6-digit EKMS ID or COMSEC Account Number of the account. If you do not have a current account number, LEAVE BLANK and the Tier 1 Registration Authority will assign your EKMS-ID.*

**b. (U) Modify Account:** Once an account is established, any adjustments to the data are considered modifications. *Establishing an AKMS account from a traditional account is not a modification; it is an establishment of a new account*. Once an account is established, any changes are considered modifications. Provide the 6-digit EKMS ID or COMSEC Account Number of the account and the reason for the modification(s).

**c. (U) Close Account:** Indicates account is to be closed. Provide the 6-digit EKMS ID or COMSEC Account Number of the account.

**4. (U) Address Information:**

**a. (U) Mailing Address and Physical Address:** Enter the COMSEC Account mailing address (please ensure to include the zip code/APO number). The physical address is the physical location of the account including: Unit Designation; ATTN: COMSEC Account (number); physical location (e.g., street address, building number, room number); city, state, and zip code or APO/FPO (OCONUS).

**b. (U) Message Address** is the AUTODIN or DMS message address of the unit/COMSEC account (i.e., AUTODIN: CDR41STSIGBN SEOUL KOREA//5AK020// or DMS Address: /C=US/O=U.S. Government/OU=DoD/OU=ARMY/OU=Organizations/L=CONUS/L=FORT HUACHUCA AZ/OU= CSLA/OU=CSLA CMD).

**c. (U) DCS Address** is the 2-line address taken from the submitting COMSEC Account's DCS Form 10.

**d. (U) Internet Protocol (IP) Address: LEAVE BLANK.** The Tier 1 Registration Authority will provide this information to the unit.

**e. (U) Highest Classification Indicator (HCI)** code defines the highest level of cryptographic material the account can receive. All accounts handling cryptographic material regardless of form (hard copy, electronic, etc.), are required to provide an HCI as defined in the following matrix:

| HCI Value | Operational Key | Seed Key |
|---|---|---|
| T | TOP SECRET | TOP SECRET |
| 1 | SECRET | TOP SECRET |
| S | SECRET | SECRET |
| 2 | CONFIDENTIAL | TOP SECRET |
| 3 | CONFIDENTIAL | SECRET |
| C | CONFIDENTIAL | CONFIDENTIAL |
| 4 | UNCLASSIFIED | TOP SECRET |
| 5 | UNCLASSIFIED | SECRET |
| 6 | UNCLASSIFIED | CONFIDENTIAL |
| U | UNCLASSIFIED | UNCLASSIFIED |

**f. (U) Special Handling Code (or Handling Indicator).** Normal Handling (NH) is the standard special handling code. The required data has been provided for you in the account registration packet.

**g. Delivery Restriction Indicator (DRI)** indicates that the COMSEC Account can receive FIREFLY Key and/or Type O/1 Key. The required data has been provided for you in the account registration packet.

**5. (U) Type of Account/EKMS ID:** This block indicates the COMSEC account's responsibilities. Check all that apply. The COMSEC Custodian will leave the Central Office of Record and Registration Authority blank. **Traditional COMSEC Account** indicates the requesting account is a non-AKMS COMSEC Account; **Controlling** Authority indicates the requesting account is a Controlling Authority of one or more short titles; **Seed Only COMSEC Acct** indicates the requesting account holds only Seed Key in their COMSEC account; **AKMS Account** indicates the requesting account is an AKMS COMSEC Account; **COMSEC Acct. already established** indicates that a COMSEC Acct (either AKMS or traditional) has been established; User **Representative** indicates that the individual submitting the registration packet is a User Representative for ordering modern key (e.g.., STU-III/SDNS); **Unclas. COMSEC Acct**. indicates that the individual submitting the registration packet holds only UNCLAS COMSEC material in their account; **EKMS ID Only** indicates that the individual submitting the registration packet has an EKMS ID but is not a COMSEC Account, Command Authority, User Rep, or Controlling Authority; and **Command Authority** indicates that the individual submitting the registration packet is a Command Authority and responsible for individual User Representatives and the DAO Codes that they are assigned.

**6. (U) Government Contract Information:** For contractor use ONLY.

**(U) Contract Number/MOA/MOU:** Enter the contract number between the U.S. Government and contractor that necessitates the need for the COMSEC account. **Expiration Date:** Enter the contract expiration date (date format is YY/MM/DD). **Commercial and Government Entity (CAGE):** If applicable, enter the CAGE Code. The CAGE code is a five-character alphanumeric.

**7. (U) Facility Security Officer (FSO):** For contractor use ONLY.

**The following fields and format are required:**
**Full Name:** Last, Mr., Miss, Mrs., Ms., First, Middle Initial.
**SSN:** xxx-xx-xxxx
**Clearance:** Personnel clearance levels such as TOP SECRET, SECRET, OR CONFIDENTIAL.
**Appointed:** Date appointed to the FSO position, numerics, YY/MM/DD.
**Signature:** FSO must provide signature.
**Grade/Rank:** Required, if applicable.
**Telephone:** The commercial telephone number is required. It must contain the 3-digit area code and at least a 7-digit telephone number.
*The DSN, secure and fax telephone numbers, and the e-mail address are optional.*

**8. (U) Account Equipment/Fill Devices/Key:**

(U) Check all items that the account currently supports or plans on supporting. For example, an account may have an LMD/KP that secures communications with a STU-III and uses a DTD to transfer key to a KG-84C. In this case, LMD, KP, KG-84C, STU-III, DTD, Seed key, Operational key and Traditional key would be checked (note that 84C would need to be typed in). Also, you may have a KG-83, KG-84, KG-75, and KG-175. If you have more equipment than space provided, list them under "other." In addition, if this is a contractor account, identify if the equipment is government-furnished, contractor-acquired, or contractor-owned property.

**9. (U) Primary Custodian/POC (AKMS):**

(U) Check the line next to Primary Custodian if you have a COMSEC account. **If registering as a CONAUTH, UR, or Command Authority, check the line next to POC (AKMS)**. Enter all information (full Name, SSN, Custodian Clearance, etc.). Next to Successfully Completed SCCC and Formally Trained on LCMS, annotate the location at which you were trained and the dates each course of instruction was completed.

(U) IT IS IMPORTANT TO NOTE THE COMSEC CUSTODIAN/ALTERNATE/CONAUTH/USER REPRESENTATIVE/COMMAND AUTHORITY MUST ALL PROVIDE SIGNATURES. UNSIGNED COMSEC ACCOUNT REGISTRATION PACKETS WILL BE RETURNED TO THE UNIT!

**10-12. (U) Alternate Custodian/Alternate POC is NOT Required for EKMS IDs**

(U) If the COMSEC account has more than three alternate custodians, add the additional alternate custodian(s) to section 21 (Additional Information) of the registration packet. **An Alternative POC is not required for EKMS IDs other than a Primary account.** Next to **Successfully Completed SCCC** and **Formally Trained on LCMS**, annotate the location at which you were trained and the dates each course of instruction was completed.

(U) IT IS IMPORTANT TO NOTE THE COMSEC CUSTODIAN/ALTERNATE/ CONAUTH/USER REPRESENTATIVE/COMMAND AUTHORITY MUST ALL PROVIDE SIGNATURES. UNSIGNED COMSEC ACCOUNT REGISTRATION PACKETS WILL BE RETURNED TO THE UNIT!

**13. (U) EKMS Information:** REQUIRED FIELD. Manual accounts disregard this entry.

(U) This field identifies the media an account can receive. Each media should be ranked in order of preference from 1 to 11. **All media listed does not have to be checked, only those that apply to the account.**

(U) The recommended order of media preference is as follows: X.400 STU-III as your first choice method of distribution, direct STU-III as your second choice, UNIX 3.5 HD as your third choice, and hard copy as your last (**at least four selections MUST be filled in**). ***The recommended order of media preference has been selected for you in the COMSEC Account Registration Packet*.

**14. (U) X.400 Address:** Manual accounts disregard this entry.

**a. (U)** Client Communications Address:

(U) EKMS Full Address: This field will identify the X.400 address used over the EKMS for electronic distribution information and key. It will be used for STU-III and KG-84 secured X.400 communications. In EKMS, the first three fields are standard **US_X_GOV+EKMS**. This information has been provided on the COMSEC Account Registration Packet.

(U) Organization Name: "**ARMY**" **will always be entered here.** The required data has been provided for you on the COMSEC Account Registration Packet. *Please DO NOT modify this information unless instructed by the Registration Authority (CSLA).*

(U) Organization Unit Name: **Enter your EKMS ID number on line #1.** Your EKMS ID number will be your current COMSEC account number. If you do not have a current COMSEC account number, LEAVE BLANK and the Tier 1 Registration Authority will assign your EKMS-ID.

**b. (U)** Server Communication Address: LEAVE BLANK. **Provided by the Tier 1 Registration Authority.**

**15. (U) Security Clearance of the Facility**:

(U) If this packet is being completed for a COMSEC account, the custodian must indicate the security level of the COMSEC Facility Approval (SECRET/TOP SECRET, etc.).

**16. (U) Date of the COMSEC Facility Approval:**

(U) Enter the date the COMSEC Facility was approved.

**17. (U) Major Army Command:**

(U) Enter the MACOM (FORSCOM, Eighth Army, USAREUR, etc.).

**18. (U) Number of Hand Receipt Holders:**

(U) Enter the number of Hand Receipt Holders for the account.

**19. (U) Commanding Officer/Designated Representative**:

(U) Enter the full name, SSN, telephone number, etc., of the Commanding Officer/Designated Representative of the unit submitting the COMSEC Account Registration Packet. IT IS IMPORTANT TO NOTE THAT THE SIGNATURE OF THE COMMANDING OFFICER/DESIGNATED REPRESENTATIVE MUST BE PROVIDED. UNSIGNED ENTRIES WILL NOT BE PROCESSED**!**

**20. (U) Next Higher Headquarters:**

(U) Enter the next higher headquarter's name, mailing address, telephone number, and e-mail address of the unit submitting the Account Registration Packet.

**21. (U) Additional Information:**

(U) Use block 21 for remarks or to provide additional information.

**22. (U) Account's DODAAC:**

(U) Enter the COMSEC Account's DODAAC. (If you don't know your DODAAC, check with your Property Book Officer [PBO]).

**23. (U) Registration Authority Information**: LEAVE BLANK.

(U) For Tier 1 Registration Authority use ONLY.

## COMSEC Account Registration Packet

Date Submitted_____ Registration Authority ID

__ __ __ __ __ __

**1. Agency Submitting Request: For Tier 1 RA use ONLY.**

Agency Name _____

Affiliation _____

__COR/Registration Authority
__ Government Agency
__ Army
__ Air Force
__NSA
__Government Contractor
__Navy/Marine/Coast Guard
__Allied

**2. Account Submitting Request:**

Agency Name _____

Affiliation ARMY

__ Active Army
__ National Guard
__ Government Contractor
__ Reserves

**3. Type of Action:**

__ a. Register New Acct No/ID__ __ __ __ __ __

__ b. Modify Acct-Acct No/ID __ __ __ __ __ __

**Reason for modification(s)**_____

_____

__ c. Close Acct-Acct No./ID__ __ __ __ __ __

**4. Address Information:**

a. Mailing Address: Physical Address:

_____ _____
_____ _____
_____ _____
_____ _____
_____ _____

b. Message Address: _____

_____

c. Defense Courier Service (DCS) Address: _____

d. Internet Protocol (IP) Address: _____

e. HCI Code___

f. Special Handling Code NH

g. Delivery Restrictions: Allowed FIREFLY key √ Yes ; Type 1 key √ Yes
Allowed KSD-64 To DTD √ Yes; Allowed Class 6 key √ Yes

**5. Type of Account/EKMS ID:**

__ Traditional COMSEC Acct.
__ Unclas. COMSEC Acct.
__ Central Office of Record
__ Registration Authority
__ Controlling Authority
__ Seed Only COMSEC Acct.
__ EKMS Account
__ User Representative
__ COMSEC Acct. already established
__ EKMS ID Only
__Command Authority



FOR OFFICIAL USE ONLY

**6. Government Contract or MOA/MOU Information: <u>For contractor use ONLY</u>.**

Contract Number/MOA/MOU*_____

Expiration Date __ __/__ __/__ __

Commercial and Government Entity Code (CAGE Code) __ __ __ __ __

Contracting officer/COR name and telephone number: _____

_____

**Attach copy of DD-254 or Memorandum of Agreement/Memorandum of Understanding*

**7. Facility Security Officer (FSO): <u>For contractor use ONLY</u>.**

Full Name _____ SSN __ __ __-__ __-__ __ __ __

Clearance _____ Appointed __ __/____/__ __

Signature _____ Grade/Rank_____

Telephone (Commercial) (_____) _____ - _____ Ext. __ __ __ __

DSN ____- _____

Secure Phone (Commercial)(_____)_____ - _____ Ext. __ __ __ __

DSN _____ - _____

Fax (_____) _____ -_____

DSN _____ - _____ STU-III __ Yes __ No

E-mail _____ _____@_____

**8. Account Equipment/Fill Device/Key (held or to be held):**

__ KG-__ __ __ __ STU-III __ KOI-18 __ Seed Key
__ KY-__ __ __ __ NES __ KYK-13 __ Operational Key
__ LMD __ CANEWARE __ KSD-64A __ Traditional Key
__ KP __ None __ DTD __ Test Key
__ Other (Specify _____
_____)
__ Government Furnished Equip. __ Contractor Owned Property
__ Contractor Acquired Prop.

**9. __ Primary Custodian/ __ POC (EKMS): (Check ONLY one)**

Full Name _____ SSN __ __ __-__ __-____ __ __

Custodian Clearance _____ Appointed __ __/____/__ __

Signature _____ Grade/Rank _____

Telephone (Commercial) (____) _____ - _____ Ext. __ __ ___ DSN _____- _____

Secure Phone (Commercial) (____) ____ - _____ Ext. __ __ ____ DSN _____ - _____

Fax (_____) _____ -_____ DSN _____ - _____ STU-III __ Yes __ No

E-mail _____@_____

Successfully Completed SCCC _____

Formally Trained on LCMS _____

**10. ___ Alternate Custodian/ ___ Alternate POC (EKMS): (Check ONLY one)**

Full Name _____ SSN __ __ __-__ __-____ __ __

Custodian Clearance _____ Appointed __ __/____/__ __

Signature _____ Grade/Rank _____

Telephone (Commercial) (____) _____ - _____ Ext. __ __ ___ DSN _____- _____

Secure Phone (Commercial) (____) ____ - _____ Ext. __ __ ____ DSN _____ - _____

Fax (_____) _____ -_____ DSN _____ - _____ STU-III __ Yes __ No

E-mail _____@_____

Successfully Completed SCCC _____

Formally Trained on LCMS _____

**11. ___ Alternate Custodian/ ___ Alternate POC (EKMS): (Check ONLY one)**

Full Name _____ SSN __ __ __-__ __-____ __ __

Custodian Clearance _____ Appointed __ __/____/__ __

Signature _____ Grade/Rank _____

Telephone (Commercial) (____) _____ - _____ Ext. __ __ ___ DSN _____- _____

Secure Phone (Commercial) (____) ____ - _____ Ext. __ __ ____ DSN _____ - _____

Fax (_____) _____ -_____ DSN _____ - _____ STU-III __ Yes __ No

E-mail _____@_____

Successfully Completed SCCC _____

Formally Trained on LCMS _____

**12. ___ Alternate Custodian/ ___ Alternate POC (EKMS): (Check ONLY one)**

Full Name _____ SSN __ __ __-__ __-____ __ __

Custodian Clearance _____ Appointed __ __/____/__ __

Signature _____ Grade/Rank _____

Telephone (Commercial) (____) _____ - _____ Ext. __ __ ___ DSN _____- _____

Secure Phone (Commercial) (____) ____ - _____ Ext. __ __ ____ DSN _____ - _____

Fax (_____) _____ -_____ DSN _____ - _____ STU-III __ Yes __ No

E-mail _____@_____

Successfully Completed SCCC _____

Formally Trained on LCMS _____

**13. EKMS Information: (MUST select at least 4 in order of preference)**
Order of media preference (numbered from 1 to 11):

| | | |
|---|---|---|
| 1 X.400 STU-III | __ X.400 KG-84 | 2 Direct STU-III |
| __ Direct KG-84 | __ UNIX 3.5 DD | 3 UNIX 3.5 HD |
| __ Tape-1600BPI | __ DOS 3.5 DD | __ DOS 3.5 HD |
| __ Tape-6250BPI | 4 Hard Copy Mechanism | |

**14. X.400 Address:**
a. Client Communication Address:
EKMS Full Address: **US_X_GOV+EKMS**

Organization Name: ARMY;_____

Organization Unit Name (Enter EKMS ID): 1. _____ 2. Do Not Use_____
3. Do Not Use_____ 4. Do Not Use_____
b. Server Communication Address:
**MTA**_____

**15. Security Clearance of the Facility:** _____

**16. Date of the COMSEC Facility Approval:**_____

**17. Major Army Command:** _____

**18. Number of Hand Receipt Holders:**
_____

**19. Commanding Officer/Designated Representative:**

Full Name _____ SSN __ __ __-__ __-__ __ __ __

Signature _____ Grade/Rank_____

Telephone (Commercial) (____) _____ - _____ Ext. __ __ __ DSN _____- _____

Fax (_____) _____ -_____ DSN _____ - _____ STU-III __ Yes __ No

E-mail _____@_____

**20. Next Higher Headquarters:**
Mailing Address:_____
_____
Telephone (Commercial) (_____)_____ EXT._____
E-Mail_____@_____

**21. Additional Information:**
_____
_____
_____
_____

**22. Account's DODAAC:** _____

**23. Registration Authority Information:** **For Tier 1 RA use ONLY.**

Signature_____

Title _____ Date_____

Telephone (__ __ __) __ __ __ - __ __ __ __ Ext. __ __ __ __

DSN __ __ __ -__ __ __ _____

Secure Phone (_ _ _) _ _ _ - _ _ _ _ Ext.__ __ __ __ DSN __ __ __- __ __ __ _____

Fax (__ __ __) __ __ __ - __ __ __ __ DSN __ __ __ - __ __ __ __ STU-III__ Yes __ No

E-mail _____@_____

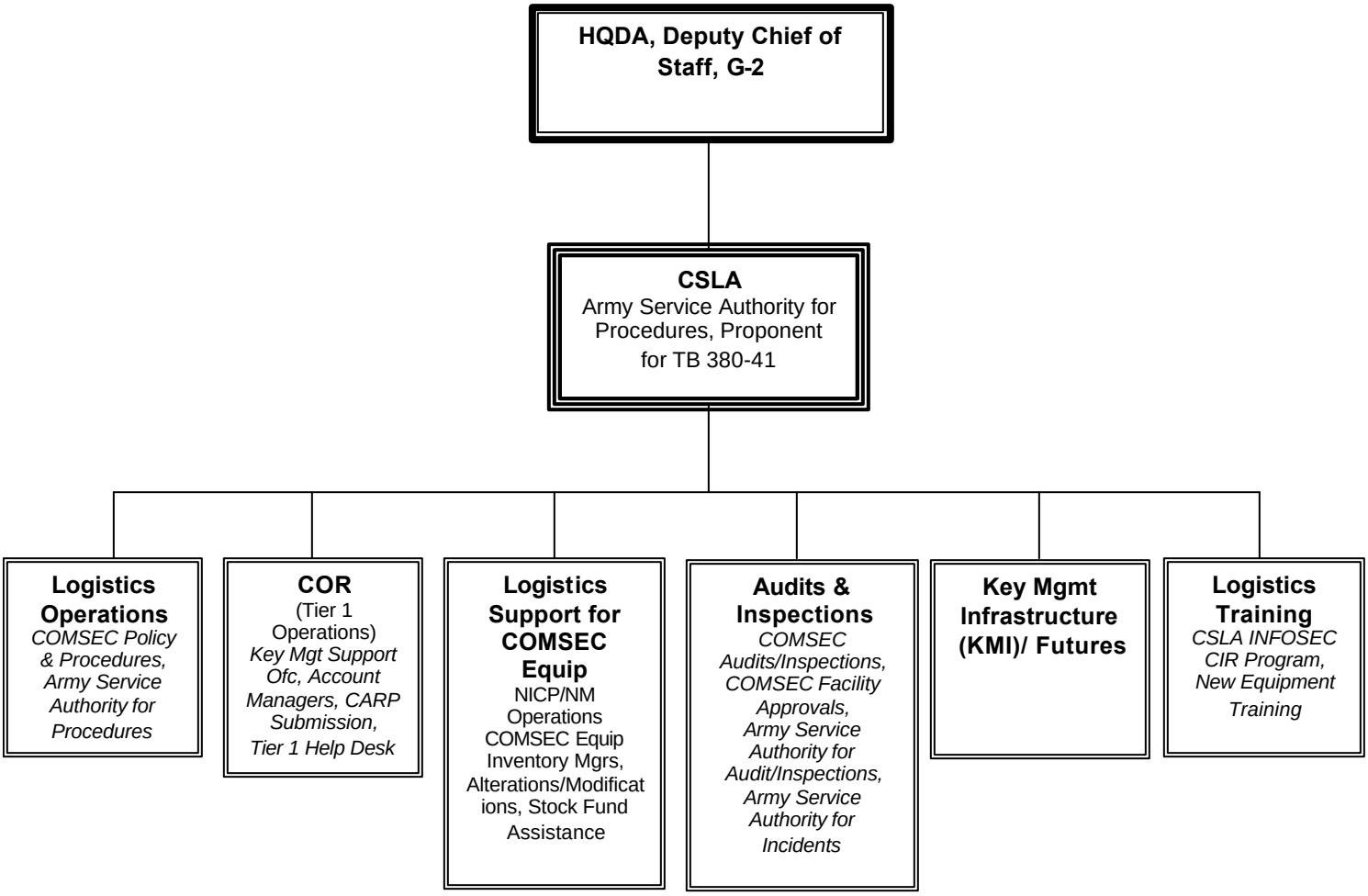
**THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY**

# APPENDIX F

# ARMY STRUCTURE FOR COMSEC SUPPORT

# COMSEC MATERIAL CONTROL SYSTEM (CMCS)

## POINTS OF CONTACT (POC)






FOR OFFICIAL USE ONLY

CSLA HELP DESK

*Telephone Number*

1-800-662-2123

TIER 1 EKMS HELP DESK
(Fort Huachuca, AZ)

*Telephone Number*

1-520-538-9900 (DSN: 879)
Toll free: 877-896-8094
(The Tier 1 Help Desk can be direct dialed or reached through the CSLA Help Desk)

TIER 1–FT HUACHUCA, AZ

*Mailing Address*

ATTN SELCL-ID-KEY/OR/EKMS
US ARMY CECOM CSLA
2133 CUSHING ST STE 3600
FORT HUACHUCA, AZ 85613-7041

*Message Addresses*

AUTODIN:

DIR TIER1 FT HUACHUCA AZ
//SELCL-ID-KEY/OR/EKMS//

DMS Address:

/C=US/O=U.S.Government/OU=DoD/OU=ARMY/OU=Organizations/L=CONUS/L=FORT HUACHUCA AZ/OU=CSLA/OU=CSLA CMD

*Telephone Numbers*

DSN: 879-8871
7068
8169
Commercial: (520) 538-(extension)

TIER 1–LACKLAND AIR FORCE BASE, TX

*Mailing Address*

USAF
US Air Force Cryptologic Depot
ATTN: CPSG
San Antonio, TX 78243-5000

*Telephone Numbers*

DSN: 969-2557

Commercial: (210) 977-2557

EXTENSION TIER 1 (ET1S)

*Mailing Address*

OIC
11th Signal Detachment
ATTN: TCMO
AP0 AE 09058-3154
(Mannheim, GE)

*Telephone Numbers*

DSN: 314-382-5835/5838
Commercial: 49-621-779-5835/5838

ADDITIONAL ASSISTANCE FOR LCMS WORKSTATIONS

Procurement assistance on HP T-20 Cartridges

| | |
|---|---|
| CONUS | 1-800-243-9812 |
| | (650) 857-3744/7048 |
| Korea | (82) 2769-0114 |
| Germany | (49) 7031-140 |

KEY MANAGEMENT

Annual key material review
Authentication Systems
Emergency requirements
Establishing Cryptonets
Exceptions
Excess/unserviceable key
Implementation of emergency plans
Key forecast requirements
Resupply due to compromised key

*Mailing Address*

ATTN SELCL-ID-KEY
US ARMY CECOM CSLA
2133 CUSHING ST STE 3600
FORT HUACHUCA, AZ 85613-7041

*Message Addresses*

AUTODIN:

DIR TIER1 FT HUACHUCA AZ
//SELCL- ID-KEY//

DMS Address:

/C=US/O=U.S.Government/OU=DoD/OU=ARMY/OU=Organizations/L=CONUS/L=FORT HUACHUCA AZ/OU=CSLA/OU=CSLA ID Key

*Telephone Numbers*

DSN: 879 - 8345
7560
8359
8337
Commercial: (520) 538-(extension)

CMCS POLICY & PROCEDURES
Resolves all procedural questions
Resolution of conflicts in TB 380-41
Submission of DA Form 2028

*Mailing Address*

ATTN SELCL-ID-P3
US ARMY CECOM CSLA
2133 CUSHING ST STE 3600
FORT HUACHUCA, AZ 85613-7041

*Message Addresses*

AUTODIN:

DIR CSLA FT HUACHUCA AZ
//SELCL-ID-P3//

DMS Address:

/C=US/O=U.S.Government/OU=DoD/O
U=ARMY/OU=Organizations/L=CONUS
/L=FORT HUACHUCA AZ/OU=
CSLA/OU=CSLA CMD

*Telephone Numbers*

DSN: 879-2332
6431
8341
Commercial: (520) 538-(extension)

COMSEC INCIDENT REPORTING
COMSEC AUDIT/INSPECTION
CARP submission
COMSEC Facility Approvals
(Fort Huachuca, AZ)

*Mailing Address*

ATTN SELCL-SAS
US ARMY CECOM CSLA
2133 CUSHING ST STE 3600
FORT HUACHUCA, AZ 85613-7041

Message Addresses
AUTODIN:

DIR CSLA FT HUACHUCA AZ
//SELCL-SAS//

DMS Address:

/C=US/O=U.S.Government/OU=DoD/
OU=ARMY/OU=Organizations/L=CON
US/L=FORT HUACHUCA AZ/OU=
CSLA/OU=CSLA CMD

INCIDENT REPORTING

*Telephone Number*

DSN: 879-6008
7519/7578
Commercial: (520) 538-extension

*Message Address*

DMS Address:

/C=US/O=U.S.Government/OU=DoD/
OU=ARMY/OU=Organizations/L=CON
US/L=FORT HUACHUCA AZ/OU=
CSLA/OU=CSLA Incidentdesk 1(uc)

AUDIT/INSPECTIONS

*Telephone Number*

DSN: 879 - 7509
7578
6722
7519
Commercial: (520) 538-(extension)

INFORMATION ASSURANCE DIV

- COMSEC Equipment Alteration/Modification
- Stock Fund Assistance (Fort Huachuca, AZ)

*Mailing Address*

ATTN SELCL-IA
US ARMY CECOM CSLA
2133 CUSHING ST STE 3600
FORT HUACHUCA, AZ 85613-7041



FOR OFFICIAL USE ONLY

*Message Addresses*

AUTODIN:

DIR CSLA FT HUACHUCA AZ
//SELCL-IA//

DMS Address:

/C=US/O=U.S.Government/OU=DoD/
OU=ARMY/OU=Organizations/L=CON
US/L=FORT HUACHUCA AZ/OU=
CSLA/OU=CSLA CMD

*Telephone Number*

1-800-662-2123

REPLACEMENT OF ID PLATES AND PCB ID LABELS
(Fort Huachuca, AZ)

*Mailing Address*

ATTN SELCL-IA-B
US ARMY CECOM CSLA
2133 CUSHING ST STE 3600
FORT HUACHUCA, AZ 85613-7041

*Message Address*

DIR CSLA FT HUACHUCA AZ
//SELCL-IA-B//

*Telephone Number*

1-800-662-2123

CSLA INFOSEC REPRESENTATIVES (CIRs)

**CONUS:**

(1) Fort Huachuca, AZ – Toll Free, 1-800-662-2123

(2) Fort Hood, TX – DSN 738-7485, Comm (254) 288-7485

(3) Fort Bragg, NC – DSN 337-2057, Comm (910) 907-2057

**OCONUS:**

(1) Europe – Heidelberg – DSN 314-375-8763, Comm (49)-0621-487-8763

(2) Europe – Stuttgart – DSN 314-421-2984 Comm (49) 0711-729-2984

(2) Korea - DSN 315-723-6237, Comm 82-2-791-33052

DIRECTOR, NATIONAL SECURITY AGENCY (NSA)
(Fort Meade, MD)

- Establishing Machine Or Auto-manual Cryptonets
- Reporting Duplicate Or Missing Numbered Key Pages

*Message Address*

DIRNSA FT MEADE MD //Y132//

*Mailing Address*

DIRNSA
ATTN Y132
Ft Meade, MD 20755-6000

- Emergency Requirement For Key.
- Requests For Resupply Of Key

*Mailing Address:*
DIRNSA
ATTN CA 880099
OPS BLDG #3, Suite 6574
FT MEADE, MD 20755

*Message Address*
DIRNSA FT GEORGE G. MEADE MD //Y13//

- COMSEC Incidents

*Message Address*

DIRNSA FT MEADE MD //I413//

*Mailing Address*

DIRNSA
ATTN I413
Ft Meade, MD 20755-6000

SERVICE AUTHORITIES

Policy – HQDA, DCS G-2, ATTN: DAMI-CD

Procedures – CSLA, ATTN: SELCL-ID-P3

Audit/Inspections – CSLA, ATTN: SELCL-SAS

Incidents – CSLA, ATTN: SELCL-SAS-IN

Assignment of COMSEC Accounts – CSLA, ATTN: COR

CONAUTH – CSLA, ATTN: Key Management

Command Authority User Representative – CSLA, ATTN: Key Management

**THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY**

# APPENDIX G

# LOCAL PRE-INSPECTION CHECKLIST

| | **DESCRIPTION OF ACTION TO BE TAKEN (THIS LIST IS NOT ALL INCLUSIVE)** |
|---|---|
| | (1) The basis for approval of the facility, as reflected in the latest memorandum, "COMSEC Facility Approval Request," remains unchanged (AR 380-40, paragraph 4-4). |
| | (2) Review Command COMSEC inspections to ensure all discrepancies indicated on previous inspection reports have been reconciled IAW AR 380-40, paragraph 6-2. |
| | (3) Have authorized systems users been assigned operator's privilege management responsibility accordingly with the account's highest security level (NAG 71, paragraph 21)? |
| | (4) Maintenance personnel have been certified on DD Form 1435 per AR 25-12, chapters 3 & 4. |
| | (5) The requirements for access to COMSEC information are known and adhered to (IAW AR 380-40, paragraphs 2-3) and clearances are verified per AR 380-67, chapter 7.<br>a. Is there an access roster posted?<br>b. For accounts that are only a safe, the access roster is the SF 700.<br>c. Is security clearance of personnel on the access roster (SF 700) equal or higher to the classification of material held? |
| | (6) The following documents are readily available or on requisition: AR 380-40, TB 380-41, AR 380-5, and AR 710-2/Unit Supply Update. |
| | (7) Personnel understand the use of the marking "CRYPTO" (paragraph 5.1.5 and AR 380-40, paragraph 2-8). CRYPTO designator identifies all COMSEC key used to protect or authenticate information. |
| | (8) For AKMS accounts, are the COMSEC Custodian and alternate LCMS Workstation-trained (IAW AR 380-40, paragraph 1-4.h(3) and TB 380-41, paragraph 2.3.1b). |
| | (9) The COMSEC Custodian and alternate custodian(s) have been appointed on a current Registration Packet (paragraph 2.3.1 and Appendix D).<br>a. Is it current and on file? |
| | (10) The COMSEC Custodian is a graduate of the Standard COMSEC Custodian Course (SCCC) (paragraph 2.3.1b and AR 380-40, paragraph 1-4.h[2]). |
| | (11) The COMSEC Custodian's other assigned duties permit sufficient time to adequately discharge their custodial duties (paragraph 2.3.1c). |
| | (12) Is there any evidence of tampering on Key Processor (Nag 71, paragraph 22-4)? |
| | (13) COMSEC records are maintained IAW paragraph 4.3 and AR 380-40, Appendix C. |
| | (14) Are there Two-Person Integrity (TPI) procedures established for accounts that will output unencrypted Top Secret key (NAG 71 22-6)? |
| | (15) All mandatory modifications to classified COMSEC equipment are applied and the equipment modification records plates accurately reflect their application IAW TB 750-38(C). |
| | (16) Procedures for checking packages upon receipt for evidence of tampering or exposure of contents are known (paragraph 4.4.3). |
| | (17) Personnel are familiar with page check requirements (paragraphs 4.4.5 and 4.4.6).<br>a. For CRYPTO-marked key, is a record of page checking (name, grade, unit, and date) posted to the Record of Page Check or the first page of the document?<br>b. For COMSEC publications, is a record of page checking posted to the Record of Page Check? |

| | |
|---|---|
| | (18) Keying material is inventoried in a manner that assures continuous protection and control (paragraph 4.12c).<br>a. Daily inventory can be verified with SF 702.<br>b. Is daily inventory taken by Hand Receipt Holders?<br>c. Is daily inventory for TS material initialed by two people? |
| | (19) Inventories of ALC 4 material are recorded on IR Cards or an SF 153 has been prepared, signed and witnessed listing all ALC 4 material held by the account (paragraph 4.13.5). |
| | (20) COMSEC material (including amendment residue) is destroyed in accordance with the schedule and procedures in chapter 6. Superseded key is completely destroyed by burning or by destruction devices and methods that meet the criteria in paragraph 4.19.<br>a. Are Local Destruction Reports signed by two properly cleared people?<br>b. Do consolidated destruction reports have back-up Local Destruction Reports? |
| | (21) COMSEC publications, as required, are posted with the latest changes and amendments and are page checked (paragraph 4.4.6, 4.15.3 and DA PAM 25-35).<br>a. Are the amendments posted within two days of receipt?<br>b. Is the Record of Amendments page completed, to include amendment identification (i.e., for hard copy: amendment number, message amendments will be DTG, and letter amendments: LTR and date)?<br>c. Were amendments posted in sequence? |
| | (22) Local accounting procedures for issuing COMSEC material are known and properly implemented (paragraph 4.16).<br>a. Are hand receipts (SF 153) properly completed?<br>b. Is electronic key being issued on a local key control document (i.e., DA Form 5941-E or DA Form 5251-E)? |
| | (23) All cryptosystems and authentication systems used by the command are NSA-approved (paragraph 3.3.4). |
| | (24) All keying material on hand is being used on a routine basis or is held for valid contingency purposes (paragraph 3.4.2).<br>a. Is key being destroyed without being used?<br>b. Can operational key be changed to a contingency key? |
| | (25) Amount of key held in the COMSEC account and at user level is restricted to the minimum required (paragraph 3.9 thru 3.9.5). |
| | (26) Are any FIREFLY credentials that have been received now expired (NAG 71, paragraph 9 and AKMS message # 5)? |
| | (27) All users know the identity and address of the CONAUTH for all key held (paragraph 2.3.2).<br>a. How does the custodian maintain CONAUTH information? |
| | (28) Has Data backup been accomplished in the event of a system failure (NAG 71 paragraph 22-c-2-a)? |
| | (29) If a secure room is used for operations, it meets the minimum requirements of paragraph 5.3.2 and AR 380-40, Appendix D.<br>a. Does the account's CFAR accurately identify what is physically in place in the facility? |
| | (30) When the COMSEC Facility is unoccupied, it is provided with safeguards that are deemed by the commander to afford proper protection against unauthorized access (paragraph 5.7).<br>a. Are locking bars being used on equipment loaded with classified key at unattended sights?<br>b. Are locking bars used on classified equipment in mobile/transportable facilities?<br>c. Are security containers securely affixed to mobile/transportable facilities? |



FOR OFFICIAL USE ONLY

| | |
|---|---|
| | (31) Unsecured telephones and other transmitting devices on site are actually required for operation (paragraph 5.3.4). |
| | (32) Only mission essential, government owned tape recorders, radios, television receivers and cameras, etc. are authorized in the operational COMSEC Facility (paragraph 5.3.5b).<br>a. Are there any personally owned electronic or duplicating devices in a operational COMSEC Facility?<br>b. Has the local commander authorized, in writing, the use of radios, TVs etc? |
| | (33) Installation and operation of electronic access control devices conform to the requirements of paragraph 5.3.5c.<br>a. Does the facility door have another approved locking device in addition to the electronic?<br>b. Has the combination been changed at least annually (recorded on an SF 700 attached to or near the door)? |
| | (34) COMSEC key is stored as required by paragraph 5.8.1.<br>a. Is TS material stored under TPI rules?<br>b. Is open storage used for classified COMSEC key? If so, is open storage authorized IAW AR 380-40, 2-21.b? |
| | (35) Location where classified CRYPTO key is stored is augmented by facilities that prevent unauthorized access to the storage container or vault itself IAW paragraph 5.8.3c.<br>a. Do COMSEC Facilities consisting of no more than a safe(s) have a second barrier, such as a key lock in the door and controlled access to the keys?<br>b. Has the TS area been declared a No-Lone-Zone?<br>c. Are there controls on visual access (i.e., drapes on windows, material in safes, inside cannot be seen from a common use area, etc.)? |
| | (36) Containers used for storing classified COMSEC information meet original procurement specifications for physical security (paragraph 5.8.3b).<br>a. Is TS material being stored in a previously damaged safe that has been restored to meet original specifications?<br>b. For SECRET and below material, has a previously damaged safe been restored to meet original specifications? |
| | (37) Locks used to secure storage containers or to secure rooms are approved built-in combination locks or, where prescribed, are approved combination padlocks commensurate with the classification of material and circumstances (paragraph 5.8, 5.11.2(d) and AR 380-40, paragraph D-3.d).<br>a. Have all safes and Group 1-type locks been modified with the new electronic combination locks (X07) IAW DA message DTG 232059Z NOV 93, SUBJECT: Retrofit Program for Security Locks?<br>b. For unattended sites, is equipment secured with locking bars and secured by an electro-mechanical lock meeting Federal Specification FF-C-2740? |
| | (38) When not installed in an operational configuration, classified crypto-equipment and components are stored securely (paragraph 5.8.4a).<br>a. Is COMSEC crypto-equipment being stored with items of monetary value (i.e., money, jewelry, etc.)?<br>b. Are common fill devices being stored keyed when not specifically authorized? |
| | (39) When installed in an operational configuration, unattended, un-keyed crypto-equipment is left installed and protected in a manner approved by the commander IAW paragraph 5.8.4b.<br>a. Is the vehicle or shelter containing the classified COMSEC equipment secured with a 5200 Series High Security Padlock or a combination lock?<br>b. Is classified COMSEC equipment secured in its shelter mounting by a steel locking bar that is locked in place with combination padlocks meeting Federal Specification FF-P-110, Sergeant & Greenleaf Model 8077A (NSN 5340-00-285-6523)? |

| | |
|---|---|
| | (40) All classified COMSEC documents are stored securely (paragraph 5.8.4e).<br>a. Are all classified documents and equipment stored in a safe?<br>b. Has the commander authorized, in writing, open storage of material classified SECRET and below (other than classified CRYPTO key)? |
| | (41) Lock combinations have been changed within the past 12 months or when an individual knowing the combination no longer requires access (AR 380-5, paragraph 5-104.b and AR 380-40, paragraph 4-5.g).<br>a. Is the SF 700 properly classified?<br>b. Is the SF 700 signed and dated?<br>c. Are there two SF 700s for TS safes? |
| | (42) Lock combinations are disseminated to an absolute minimum number of authorized personnel (paragraph 5.8.4h(3)). |
| | (43) Access to the COMSEC Facility is granted and controlled IAW the provisions of paragraph 5.2a and AR 380-40, paragraph 4-5.d.<br>a. Is there a COMSEC Facility access roster posted or on file in the account?<br>b. Do the people having access have the appropriate security clearances?<br>c. Are visitors required to sign the Restricted Area Visitors Register (DA Form 1999-E)?<br>d. Is the DA Form 1999-E signed by the authorizing official and IN/OUT times recorded? |
| | (44) Daily security checks are made at the end of each workday and on non-workdays, as required (paragraph 5.4.1 and 5.4.2).<br>a. If the COMSEC Facility is a room/building, is an SF 701 being maintained?<br>b. Is the SF 702 being maintained correctly (i.e., "checked by" block always filled out, whether opened or not; not required if the room is not entered)? (The "checked by" block can be initialed by the same person that locked the safe, if no one else is available.)<br>c. For TS safes, are there two SF 702s: one for each combination? |
| | (45) The procedures for preparing classified COMSEC material for shipment are known and adhered to (paragraph 5.10.1). |
| | (46) Authorized means of transporting classified COMSEC material are known and adhered to (paragraph 5.10.2 and AR 380-40, paragraph 2-17). |
| | (47) Where applicable, an emergency plan has been prepared and includes those provisions of paragraph 5.16.1 deemed appropriate by the commander (AR 380-40, paragraph 3-4).<br>a. For OCONUS accounts, is there an emergency plan prepared?<br>b. Is the plan workable (i.e., how/where are safe combinations located, how do you carry large quantities of COMSEC material, where do you get a vehicle, how do you start a fire, etc.)? |
| | (48) The emergency plan is compatible with command emergency plans (paragraph 5.16.2), and emergency procedures provide for the immediate destruction of superseded key IAW paragraph 5.18.5.<br>a. Has the emergency plan been coordinated with those units involved? |
| | (49) Emergency destruction materials are adequate and readily available for use (paragraph 5.18.5).<br>a. Are the destruction devices located where the emergency plan indicates they are? |
| | (50) Where applicable, briefings and dry runs are held quarterly (and documented), and all personnel are aware of their responsibilities in the event of an emergency (AR 380-40, paragraph 3-5 and TB 380-41, paragraph 5.15b).<br>a. Are there at least four dry run documents on file? |

| | |
|---|---|
| | (51) Sensitive pages of COMSEC maintenance manuals (KAMs) have been prepared for quick removal, where required, and personnel are familiar with the emergency implementing procedures (paragraph 5.19).<br>a. Have the upper corners of sensitive pages been cut off? |
| | (52) Personnel are familiar with reportable incidents pertaining to the cryptosystems and associated material held (paragraph 7.1 and AR 380-40, paragraph 7-3).<br>a. Is destruction documentation properly filled out, to include two signatures?<br>b. Has keying material been destroyed within 72 hours of supersession?<br>c. Is classified material properly secured?<br>d. Do users have proper security clearances for material being used? |
| | (53) Supervisory personnel are thoroughly familiar with the requirements for reporting incidents (paragraph 7.1 and AR 380-40, paragraph 7-6). |
| | (54) Users are aware of the requirement to report directly to the appropriate CONAUTH all circumstances, occurrences, or acts that could lead to a compromise of key (paragraph 7.1 and AR 380-40, paragraph 7-1).<br>a. Do COMSEC personnel know who the CONAUTH is for the material held?<br>b. Is the COMSEC Custodian the CONAUTH for any of the material held? |
| | (55) All centrally accountable COMSEC material on hand, including the number of copies or items, is mission essential (AR 380-40, paragraph 5-3).<br>a. Is the COMSEC Custodian conducting an annual review of key being held?<br>b. Is there any key being destroyed on a monthly base that is not being used? |
| | (56) Are the key processor and removable hard drive being properly stored in an approved storage area or GSA security container (NAG 71, paragraph 25)? |
| | (57) In COMSEC Facilities with a continuous (24-hour) operation, the SF 702 is properly annotated at the end of each shift change (TB 380-41, paragraph 5.4.1c).<br>a. Is the "checked by" block being annotated on the SF 702 for each shift change? |
| | (58) All personnel, whose duties require them to be in the DACAP IAW AR 380-40, Chapter 8, have received the DACAP briefing and have read and signed their DACAP certification memorandum.<br>a. A roster of all personnel assigned who are enrolled in DACAP has been forwarded to the appropriate local security office.<br>b. Personnel that no longer qualify for DACAP have signed the termination of access portion of the DACAP certification memorandum and a copy of their memo has been forwarded to the appropriate local security office. |
| | (59) Annual review by CONAUTH is accomplished and the required documentation is on hand (TB 380-41, paragraph 3.6.7a).<br>a. Is the report for the annual review of key on file in the account? |
| | (60) Is the LMD/KP connected to a Local Area Network (LAN) (NAG 71, paragraph 12-d)? |
| | (61) Are procedures in place to terminate systems access for individuals that are relieved or have departed the unit (NAG 71, paragraph 11)? |

**THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY**

# INDEX


**A**

Absence of COMSEC custodian..... 2-13, 2-14, 4-27
Access
LMD/KP ..... 6-8
Unauthorized
Compromises and Incidents (Physical)..... 7-1
Access to a COMSEC Facility .....2-11, 4-44, 4-54, 5-4
Classification level ..... 5-4
Guards ..... 5-7
Safeguarding ..... 5-6
Unauthorized ..... 5-10
Unauthorized Access
prevention ..... 5-10
Unauthorized Access During Emergency
Evacuation ..... 5-19
Unescorted access..... 5-7
Access to CCI ..... 5-3
Access to Code Combinations..... 5-6
Access to COMSEC Equipment
Unauthorized Access ..... 5-10. *See* Emergency
Access to CRYPTO Key ..... 5-2
Access to Sample Task Cards..... 5-19
Access, definition of..... 5-3
Access, Electronic Control Devices ..... 5-5
Accounting Legend Codes (ALC) .... 2-14. ***See* Chapter 4, section 4.2**
COMSEC Aid Items Register for ALC1 .....4-16
COMSEC AId Items Register for ALC4 .....4- 17
Local Accounting ..... 4-31
Transfer Report..... 2-16
Accounting Legend Codes, definition of..... 3-1
Addresses
CMCS ..... *See* CMCS Addresses
COMSEC Directory Service..... *See* COMSEC
Directory Service
DCS ..... 2-6
POC..... *See* Appendix F
AKMS..... 6-1
Account Inventory ..... ***See* Inventory**
Electronic Key Destruction ..... 6-8
Electronic Key Distribution..... 6-7
LCMS Workstation ..... 6-1
Inventory Requirements ..... 6-2
LCMS Workstation Accountability..... 6-2
Alternate COMSEC Custodians
Procedures to Change *See* COMSEC Custodian
and Alternates:Procedures to Change
Amendments
Accounting and Entering/COMSEC
Publications ..... 4-45
COMSEC Material ..... 3-3
Page-Checking ..... 4-9
Area
MEVA ..... 4-50
Security .... ***See* Access to a COMSEC Facility**
Audit
Inspection of COMSEC Accounts ..... 4-54
Physical Inventory of Key Segments ..... 4-24
Report ..... 4-55
Unknown Serial Numbers ..... 3-4
Use of IR Cards ..... 4-14
Authentication Systems ..... 3-5

**B**

Backorder..... B-5
Backorder Release..... B-5

**C**

CARP..... 4. *See* COMSEC Account
CCI ..... 3-3, 7-11
Classification of..... 5-3
Storage of ..... 5-10
CCIR ..... 6-4
& a Modified CARP ..... 2-9
& SIR ..... 6-3
AKMS Accounts..... 4-43, 6-2
Exception to Voucher Numbers ..... 4-11
HRH Material Transfer..... 6-5
Inventory ..... 4-34
Serving as an SAIR ..... 4-43
Traditional Accounts..... 4-42
Validity of ..... 4-42
Certificate of Verification ..... 6-2
CIIC..... 3-1
Classification
Duration ..... 5-3
Guidance..... 5-3
of COMSEC Key ..... 3-19
Clearance
Access to CCI..... *See* CCI
ALC
Need-to-Know..... 4-31
from COMSEC Custodial Responsibilities ... 2-15
of COMSEC Custodians and Alternates ..... 2-11
of COMSEC Witness..... 2-13




FOR OFFICIAL USE ONLY

of Couriers.....5-16
of Former COMSEC Custodian Memorandum 4-
.....43
of Guards .....5-7
of Maintenance Personnel .....5-4
of Personnel Involved in Destroying Key.....4-51
Revocation
AWOL .....7-12
Revocation or Suspension for Cause.....7-13
Status
Unauthorized Access .....*See* Physical Incidents
to CRYPTO Key.....*See* Access to Crypto Key
to Un-keyed CCI .....*See* Access to CCI
Clearance, Security
Access to COMSEC Facilities .....5-4
CMCS .....2-1
Accountability
Relief from .....7-15
Addresses
Defense Courier Service ..... 2-5
Internet Protocol (IP) .....2-6
Mailing .....2-5
Message .....2-5
Physical Location .....2-5
Architecture .....2-1
Army Structure.....2-3
EKMS ID .....2-5
Tier 1 .....2-4
Tier 2 .....2-4
Tier 3 .....2-4
as a Service Authority .....1-3
Relief from Property Accountability.....7-15
Compromises.....7-1
and Incidents, COMSEC ..... 7-1
Control
CONAUTH .....3-14
Key Material .....3-16
Marking Messages .....7-15
Restricting
User Holdings of Key Material.....3-23
Reviewing Messages .....7-14
COMSEC Account
CARP .....2-8
CFAR .....2-10
Change of Account Number.....2-8
Closing of ..... 2-16
Establishing .....2-8
Inventory of .....*See* Inventory
Movement of ..... 2-15
Number ID Structure .....2-8
Number of Accounts.....2-8
Numbering System.....2-8
Reports
CCIR.....4-43
SAIR .....4-39
Unit Deployment ..... 2-19
CSLA Responsibilities .....2-21
COMSEC Compromises and Incidents
COMSEC Incident .....7-1
Cryptographic Incidents.....7-1
Personnel Incidents.....7-1
Physical Incidents .....7-1
COMSEC Custodian
Absence ..... 2-14
Alterna te .2-13. **See also COMSEC Custodian and Alternates**
Discrepancies .....2-14
Responsibilities .....2-12
COMSEC Custodian and Alternates
Access Requirements .....2-11
Appointments .....2-11
Custodial Obligations .....2-12
Duties .....2-12
LCMS Operator Training.....6-12
Rank or Grade Requirements .....2-11
Relief from Accountability .....2-15
Training .....2-12
COMSEC Directory Service.....2-6
COMSEC Equipment
Adhesive Labels on .....4-49
Destruction of *See* also Emergency: Destruction
Storage
Unattended.....5-8
Unclassified Equipment .....3-3
COMSEC Facility
Access ..... ***See* Access to a COMSEC Facility**
Approval for HRH.....2-6
Approvals .....2-6
Approving Office .....2-6
Devices Used Within .....5-5
Downgrading .....2-6
Duration of Approval .....2-7
Establishing .....2-8
Identification .....5-4
Non-Continuous Operations.....5-6
Protecttion..... 5-3, 5-5
Mobile and Transportable ..... 5-6
Request for Approval.....2-7
Supervision of.....2-11
COMSEC Incident
Reports ..... *See* Files, Forms, and Reports
Routing of.....7-7
COMSEC Incidents.....7-1
Compromising Emanations .....7-9
Cryptographic, Unauthorized Cryptoperiod
Extension .....7-13



FOR OFFICIAL USE ONLY

Discovery of Listening Devices .....7-9
Investigations .....7-14
Personnel, Absence .....7-12
Personnel, Captured or Presumed Captured.. 7-
.....12
Personnel, CI Interview .....7-12
Personnel, Defection or Subversive Intent ..7-13
Reportable ..... 7-2
Reporting Addresees ..... 7-8, 7 -9
Reporting of.....7-4
Controlling Authority Limitations .....7-6
Reporting Responsibilities .....7-5
Reports Involving Joint-Staff Position Control
Material .....7-7
Reports Regarding Satellites and Space
Vehicles .....7-7
Satellites, Lost Material Aboard.....7-11
Unauthorized Photography .....7-11
COMSEC Key
AKMS .....*See* AKMS: Electronic Key
Authorization to Receive.....3-18
Authorized Exposure.....4-23
Availability .....3-19
Classification of.....3-19
Control of Tape Segments .....4-21
Emergency Requirements .....3-24
Excess and Unserviceable Key .....3-18
Initial Issue .....3-18
Local Accounting .....4-21
Physical Accounting for Used Segments.....4-23
Premature Exposure .....4-23
Processing Requests for.....3-19
Resupply Procedures .....3-18
Shipment of Physical Key .....3-18
Transfer Reports.....3-18
User Holdings .....3-23
Exceptions.....3-23
COMSEC Material
AKMS Account Voucher Numbers .....*See*
Voucher:Numbers
Destruction Exceptions..... 4-50
Destruction of ..... 4-49
Destruction of Other Material .....4-53
Destruction of Paper-Based Material .....4-51
Destruction Procedures .....4-51
Equipment Modification .....4-49
Hand Receipting of.....4-32
Identification of ..... 3-1
Inspection.....4-8
Inventory Prior to Transfer or Destruction of4-35
Item Register (IR) Cards .....4-14
Local Accounting *See* Hand Receipt: Holder and
Hand Receipts
Report (SF 153).....4-26
Reproduction of .....4-47
Request for Key Tapes .....3-10
Requisitioning of (and Applicable Publications)
.....3-3
Shipment..... 5-12, 5-13
Shipment of CRYPTO ..... 5-12
**Storage** .....**5-8**
Storage Containers .....5-9
Storage of CONFIDENTIAL .....5-9
Storage of CRYPTO.....5-8
Storage of SECRET.....5-9
Storage of TOP SECRET .....5-8
Storage of Unclassified.....5-9
Storage Restrictions .....5-9
Traditional Account Voucher Numbers.....*See*
Voucher:Numbers
Transfer of between COMSEC Accounts ....4-31
Voucher Control Registers .....4-12
COMSEC Witness.....**See Clearance of**
**Duties** .....2-12
CONAUTH .....3-13
Assignment of CONAUTH Duties .....3-13
Contingency Operations .....3-13
Designating Contingency Keying Material ...3-18
Determining Copy Count Requirements.....3-23
Key Material Compromises .. *See* Compromises:
Key Material
Key Material Reviews .....3-17
Logistics Support .....3-15
Management Responsibilities .....3-13
Operational Responsibilities.....3-14
Reporting Defective Keying Material.....3-17
Transfer of CONAUTH Duties .....3-13
Conversion Report .....4-7. *See* also Files, Forms, and
Reports. *See* SF 153
Voucher Numbers .....4-14
Couriers
Requirements ..... *See* Clearance of Couriers
Responsibilities .....5-16
CRYPTO
Access.....*See* Access to CRYPTO Key
Caveat .....5-2
Production of Physical Key .....5-2
Crypto-equipment
Destruction of .....5-24
Installation of (On-line) .....5-5
Quantity .....3-7
Screening from View .....5-4
Special Cabinets for .....5-11
Cryptographic Incidents..... 7-1, 7-13
Cryptologic Media .....5-16
Cryptonets



FOR OFFICIAL USE ONLY

Elements ..... 3-5
**Establishing** ..... **3-6**
Expansion of..... 3-6
Size ..... 3-6
Types of ..... 3-6
**Cryptosystems** ..... *See* also Authentication Systems
**The Need for** ..... **3-5**

**D**

DA Form 2653-E..... 4-37
Destruction..... *See* COMSEC Material: Destruction
COMSEC Maintenance Manuals..... 5-2
Emergency
Methods and Materials. .....***See* Emergency: Destruction**
Discrepancies..... *See* COMSEC Custodian
Audit Rating..... 4-55
Audit Report ..... 4-55
Hand Receipt Holder.. *See* Hand Receipt Holder
Reporting ..... 4-8
Unresolved ..... *See* Clearance: from COMSEC Custodial Responsibilities

**E**

EKMS ID..... *See* CMCS: Army Structure
Emergency
Actions Afterwards ..... 5-27
Destruction ..... 5-20, 5-24
Destruction Methods and Materials ..... 5-20
Destruction of CRYPTO Equipment ..... 5-24
Measures ..... 5-19
Plan Preparation ..... 5-17
Plans and Procedures..... 5-17
Requirements for Key ..... 3-24
Task Cards ..... 5-18
Unauthorized Access to COMSEC Equipment 5-20
Equipment Alteration..... *See* COMSEC Material
Equipment and Components
COMSEC ..... ***See* also COMSEC Material**
Storage of COMSEC .. ***See* COMSEC Material: Storage**
Evaluations
COMSEC Incident Reports .... *See* Files, Forms, and Reports: COMSEC Incident Reports

**F**

Files ..... 4-2
Files, Forms, and Reports
COMSEC Incident Reports ..... 7-6
Evaluations ..... 7-14
COMSEC Incident Reports, Amplifying ..... 7-6
COMSEC Incident Reports, Final ..... 7-6
COMSEC Incident Reports, Initial ..... 7-6
COMSEC Incident Reports, Report Precedence ..... 7-6
COMSEC Incident Reports, Reporting Incidents ..... 7-6
COMSEC Incident Reports, Routing of..... 7-7
COMSEC Incident Reports, Transmission During Minimize and In-the-Clear..... 7-9
Conversion Report ..... 4-44
Guidance..... 4
Personnel Incident Reports..... 7-12
Physical Incident Reports ..... 7-9
SAIR ..... 4-39
SF 153 *See* also SF 153 and COMSEC Material: Report
Special Possession Report ..... 4-45
Foreign Release
COMSEC Information..... 5-1
Release Prefix ..... 5-1
Requests for..... 3-13
Forms
Availability of ..... 1-1
Files, Forms, and Reports .....***See* also Files**
Reference Regulations and Forms ..... A-1
Reproducible ..... 7-E
FOUO
Application..... 5-1
Standard Request Form ..... 3-6
Funding
Assistance..... 3-3
Codes ..... 2-9
Requisitions ..... 3-1
Returns ..... 3-2

**G**

Guards
Use of ..... 5-7

**H**

Hand Receipt
Holder ..... 6-5
COMSEC Facility Approval ..... 2-6
Inventory Maintenance ..... 6-5
Holder Accounting for Superceded Key ..... 6-5
Holder Discrepancies ..... 6-5
Holder Material Transfer..... 6-5
Holder Responsibilities ..... 2-5
Numbers (Local Element) ..... 2-8
of COMSEC Material..... 4-32
Tier 3

COMSEC Hand Receipt Holder ..... 2-4
Hand Receipts ..... 6-5
Accountable Summaries ..... 6-5
Issue of ALC-4 Material Within AKMS ..... 6-6
Manual HRs ..... 6-5
Recording STU III Key Conversions in AKMS 6-6

**I**

Identification Plates ..... 3-4
Lost, Damaged, Destroyed, etc. ..... 3-4
Incidents
COMSEC ..... 7-6
Cryptographic ..... 7-13
Personnel ..... 7-12
Physical ..... 7-9
Inventory
AKMS Account ..... 6-13
CCIR or SAIR ..... 4-34
COMSEC Accounts ..... 4-34
LCMS Workstation ..... *See* AKMS: LCMS Workstation
Maintenance ..... *See* Hand Receipt: Holder: Inventory Maintenance
Physical Material ..... 4-34
Transfer or Prior to Destruction of COMSEC Material ..... 4-35
Investigations
COMSEC Incidents ..... 7-14
Item Register (IR) Cards ..... 4-14

**L**

Labels on COMSEC Equipment ..... 4-49
LCMS Workstation ..... *See* AKMS
Army Publications ..... 6-12
Maintenance ..... 6-12
Storage of ..... 6-11
LMD/KP ..... *See* also Access: LMD/KP
CIK and PIN Number Storage ..... 6-8
Disaster Recovery Kit ..... 6-8

**P**

Personnel Incidents ..... 7-1, 7-12
Reports ..... *See* Files, Forms, and Reports
Physical Incidents ..... 7-1
Clearance Status
Unauthorized Access ..... 7-10
Reports ..... *See* Files, Forms, and Reports
Publications
Army COMSEC ..... 3-3
LCMS Workstation ..... 6-12
NSA Limited Maintenance Manuals ..... 3-4
NSA-Published Policy and Doctrine ..... 3-4

**R**

Reports .. ..... ***See* Files, Forms, and Reports**

**S**

SAIR ..... 4-41
SF 153 ..... 4-30
Completion Instructions ..... 4-26
General Information ..... 4-26
Transfer Reports ..... 4-8
Shipment ..... *See* COMSEC Material: Shipment
Special Possession Report ... *See* Files, Forms, and Reports
Storage ..... *See* COMSEC Material: Storage
LCMS Workstation ..... 6-11

**T**

Tier 1 ..... *See* CMCS: Army Structure
Tier 2 ..... *See* CMCS: Army Structure
Tier 3 ..... *See* CMCS: Army Structure
Transportation ..... *See* COMSEC Material: Shipment

**V**

Verification
Certificate of ..... 6-2
Voucher
Control Registers ..... 4-12
Number
Five Digit Outgoing ..... 6-7
Numbers
AKMS Account ..... 4-10
Special Possession and Conversion Report 4-14
Traditional Accounts ..... 4-11
Numbers, Exception to ..... *See* CCIR: Exception



FOR OFFICIAL USE ONLY

By Order of the Secretary of the Army:

JOHN M. KEANE
*General, United States Army*
*Chief of Staff*

Official:

JOEL B. HUDSON
*Administrative Assistant to the*
*Secretary of the Army*

PIN 080958-000