Headquarters
United States Army, Europe, and Seventh Army
United States Army Installation Management Agency
Europe Region Office
Heidelberg, Germany

Army in Europe
Regulation 380-40*

10 July 2003

Security

Safeguarding and Controlling Communications Security Material

***This regulation supersedes AE Regulation 380-40, 2 May 2003.**

For the CG, USAREUR/7A:

MICHAEL L. DODSON
Lieutenant General, USA
Deputy Commanding General/
Chief of Staff

Official:

GARY C. MILLER
Regional Chief Information
Officer - Europe

Summary. This regulation establishes policy and prescribes procedures for safeguarding, controlling, and disposing of communications security (COMSEC) material in the European region.

Summary of Change. This revision provides updated procedures for controlling secure cellphones in private quarters (para 13c).

Applicability. This regulation applies to organizations supported by USAREUR that handle COMSEC material. The policy and procedures in this regulation apply down to company level.

Supplementation. Commanders will not supplement this regulation without USAREUR G2 (AEAGB-SAD-S) approval.

Forms. This regulation prescribes AE Form 380-40A, AE Form 380-40B, AE Form 380-40C, AE Form 380-40D, and AE Form 380-40E. AE and higher-level forms are available through the Army in Europe Publishing System (AEPUBS).

Records Management. Records created as a result of processes prescribed by this regulation must be identified, maintained, and disposed of according to AR 25-400-2. File numbers and descriptions are available on the Army Records Information Management System website at *https://www.arims.army.mil*.

Suggested Improvements. The proponent of this regulation is the USAREUR G2 (AEAGB-SAD-S, DSN 370-7214). Users may suggest improvements to this regulation by sending DA Form 2028 to the USAREUR G2 (AEAGB-SAD-S), Unit 29351, APO AE 09014-9351.

Distribution. B (AEPUBS).

CONTENTS

---

1. PURPOSE

This regulation prescribes policy and assigns responsibilities for safeguarding and controlling communications security (COMSEC) material in the European region. This regulation also provides guidance on the use of KOV-14 cards in the European region and guidance on the secure telephone unit, third generation (STU-III), program and installation of STU-IIIs, secure telephone equipment (STE), and Timeport 280 Global System for Mobile Communications-Security Module (GSM-SM) (secure cellphones) in private quarters. This regulation must be used with--

a. AR 380-19.

b. AR 380-40.

c. DA Pamphlet 25-16.

d. DA Pamphlet 25-380-2.

e. Technical Bulletin (TB) 380-41.

f. AE Pamphlet 380-40.

2. REFERENCES

Appendix A lists publications and forms.

3. EXPLANATION OF ABBREVIATIONS AND TERMS
The glossary defines abbreviations and terms.

4. RESPONSIBILITIES

a. The USAREUR G2 will--

(1) Establish policy and approve procedures for--

(a) Safeguarding and controlling COMSEC material in the European region.

(b) Conducting command COMSEC-facility inspections.

(2) Be the proponent for the Standardized COMSEC Custodian Course (INT 34), the Local COMSEC Management Software (LCMS) Course (INT 35), and the final authority in the European region for--

(a) Validating annual training needs (UR 350-1-2).

(b) Deciding on requests for approval to attend the INT-34 and INT-35 courses if established quotas are filled.

(c) Deciding on requests for approval to waive course prerequisites.

(3) Review and approve or deny requests to appoint custodians and alternates who do not meet the rank or grade requirement.

(4) In coordination with the USAREUR G3 and the USAREUR G6, review and approve or deny requests to install and use STU-III, STE, and Timeport 280 GSM-SM (secure cellphone) in private quarters (app B).

(5) Manage the Department of the Army Cryptographic Access Program (DACAP) in the European region by--

(a) Maintaining the DACAP database.

(b) Randomly selecting lists of personnel to receive the counterintelligence scope polygraph examination and provide these lists to supporting United States Army Intelligence and Security Command (INSCOM) polygraph detachments.

(c) Monitoring the DACAP and ensuring unit DACAP POCs provide monthly reports of eligible personnel (requirement control symbol (RCS): AEAGB-380-40) (Department of the Army Cryptographic Access Program).

(6) Prepare and issue COMSEC-incident trends.

(7) Appoint a command COMSEC inspector.

(8) Conduct command COMSEC inspections of European region commands.

(9) Review and approve or deny the transportation of COMSEC keying material by a U.S.-flag carrier or foreign commercial aircraft.

(10) Review and approve requests for exceptions to two-person integrity (TPI) in specific cases when compelling operational requirements warrant approval.

(11) Review and approve or deny requests for exceptions to DA policy on controlled cryptographic items (CCIs) (app C).

b. The USAREUR G3 will--

(1) In coordination with the G2 and the G6, review and approve or deny requests to validate the installation of STU-IIIs, STE, or Timeport 280 GSM-SM (secure cellphones) in private quarters (app B).

(2) Set priorities for distributing COMSEC equipment and CCIs (app C).

c. The USAREUR G4 will--

(1) Perform CG, USAREUR/7A, responsibilities under the Unique Item Tracking (UIT) Program (AR 710-3).

(2) Act as the lead for resolving COMSEC incidents involving CCIs at depots and other logistic facilities in the European region (app C).

(3) Ensure property book officers (PBOs) and other logistic personnel who handle CCIs are aware of security controls and serial-number accounting requirements (AR 710-2).

(4) Be the staff proponent for property accountability of CCI.

d. The USAREUR G6 will--

(1) Develop and publish COMSEC procedures for enforcing information systems security policy.

(2) Help develop Army in Europe COMSEC policy.

(3) Develop and publish procedures for command inspections of COMSEC facilities in the European region.

(4) Review COMSEC-incident reports (para 12) for effects on operations and provide guidance on recovery actions. Revise or develop procedures to improve security and prevent incidents.

(5) Coordinate with the G2 before issuing guidance from DOD, HQDA, and national organizations responsible for COMSEC.

(6) Distribute, in coordination with HQDA, instructions on the disposal of CCIs (app C).

(7) Be the proponent for fielding tactical cryptographic systems and ensure that users order and receive cryptographic key required to establish secure communications.

(8) Be the designated command authority POC for cryptoignition keys (CIKs) in the European region.

(9) Be the designated national distribution authority (NDA) for U.S. users of NATO COMSEC material.

(10) Be the validation authority for new manual cryptosystems.

(11) In coordination with the G2 and the G3, review and approve or deny requests to validate the installation of STU-IIIs in private residences (app B).

(12) Provide technical assistance in developing key-management guidance for user-operated equipment in the European region.

(13) Provide technical assistance to organizations in the European region on over-the-air-rekeying (OTAR) operations and techniques.

(14) Advise controlling authorities (CONAUTHs) in the European region on COMSEC supply-support procedures.

(15) Develop COMSEC logistic- and maintenance-support plans to support mobilizations, contingencies, and emergency operations conducted in the USEUCOM area of operations.

(16) Represent the European region at COMSEC logistic-, maintenance-, management-, and supply-support conferences, meetings, seminars, and working groups as directed.

e. The Commander, 11th Signal Detachment, Theater Communications Security Logistic Support Center, Europe, will--

(1) Provide specialized repair service for the theater, off-site general support (GS) maintenance, and limited (regional) direct support (DS) maintenance support for B16 source-of-supply items in the European region.

(2) Manage the United States Army Theater Communications Security Management Office, Europe (TCMO-E), as the theater COMSEC logistic support facility for storage and distribution of cryptographic key and classified COMSEC Material Control System (CMCS) hardware.

(3) Provide theater GS/DS COMSEC logistic (supply) support to the European region, other military departments, U.S. Government agencies, NATO, and other allies. This requires providing--

(a) Centralized management and stock control of operational, reserve, and contingency cryptosystems and CMCS-controlled hardware.

(b) COMSEC-supply support for cryptonets required for operations in the European region.

(c) NDA-logistic management and NDA-supply support for NATO cryptographic systems required by U.S. Forces to support NATO. Coordinate and perform national transfers among organizations in the European region, Allied Command Europe, and other allied NDAs.

(d) A centralized source for locally generated key for over-the-air-key distribution (OTAD) based on procedures in NAG-16.

(e) Management and distribution procedures to support routine and contingency operations.

(f) A centralized storage and distribution point for positive-controlled material to support USEUCOM and other Army organizations in the European region.

f. Commanders supported by a U.S. Army COMSEC account will exercise responsibilities in AR 380-40, paragraphs 1-4h, and--

(1) Maintain a current record of personnel who require access to Top Secret (TS) cryptographic key and--

(a) Report this information through the DACAP POC to the USAREUR G2 (AEAGB-SAD-S), Unit 29351, APO AE 09014-9351.

(b) Send an updated report once a month to the G2 the address in (a) above. Negative reports are required.

(c) To prevent compromise, commanders of organizations with TS COMSEC accounts should not appoint any person to the position of COMSEC custodian or alternate COMSEC custodian who does not possess a final TS security clearance.

(2) Ensure that unused quotas for the INT-34 and INT-35 courses are returned through command channels.

(3) Send operational-necessity requests for approval to transport COMSEC material by courier aboard a commercial carrier to CDRUSAREUR DCSINT HEIDELBERG GE//AEAGB-SAD-S// or to the USAREUR G2 (AEAGB-SAD-S), Unit 29351, APO AE 09014-9351.

g. The Commander, 21st Theater Support Command, will track CCI property (AR 710-3, chap 4) in the European region.

5. RESOLVING CONFLICTS

a. Commanders should refer to DA and Army in Europe policy for guidance on specific COMSEC issues or practices.

b. In cases of conflict between this regulation and other regulations, the procedures that provide a higher degree of security or control will be used until the conflict is resolved.

c. Commanders will send requests to resolve conflicts through command channels to the USAREUR G2 (AEAGB-SAD-S), Unit 29351, APO AE 09014-9351.

6. CONTROL AND MANAGEMENT OF CRYPTOKEY

a. The control and protection of TS cryptokey will be according to AR 380-40, with the following exceptions:

(1) When not stored according to AR 380-5, AR 380-40, and this regulation, TS cryptokey will be handled according to TPI rules (that is, in the possession of two persons cleared for access to the material).

(a) Key locks may be used in operational areas to store an operational cryptokey only when the facility is a "no-lone zone."

(b) If the method of storage in (a) above is used, a "RED" and "BLUE" team concept will be developed (AE Pam 380-40).

(2) SF 702 will be used on each container. If the container is used to store TPI material, the words "RED" and "BLUE" will be printed at the top of the form to show which side of the form each team initials for its particular control function. AE Pamphlet 380-40 provides exact procedures for use of the SF 702 for the X-07 and X-08 lock.

(3) An inventory should be conducted when a container is opened. An inventory must be conducted before locking a container or before going off shift in a 24-hour operation.

(a) The inventory must include checking expiration dates of key and recording the results on an adjusted DA Form 2653-R.

(b) Two sets of initials are required (except at COMSEC material direct support activities (TB 380-41)).

(c) If applicable, positive-control material must be inventoried according to Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3260.01.

(4) SF 700 must be used as specified in AR 380-5, paragraph 7-8c.

(5) Personnel with access to TS cryptokey will be enrolled in the DACAP.

b. The management of all other cryptokey must be done with AE Form 380-40C as prescribed in AE Pamphlet 380-40.

c. The following is a clarification of AR 380-40, paragraph 5-7, and TB 380-41, paragraphs 4.11.2(b)(1b) and 4.22:

(1) Key tape segments from canisters containing more than one segment of the same key will be destroyed immediately after a successful load (canister containing five segments with each segment containing the same key). If for any reason the key is zeroized (for example, machine malfunction), the second segment will be pulled and loaded. This can be repeated through segment 4. If segment 5 is pulled for use, then this segment may be held until the last day of the cryptoperiod and then destroyed within 12 hours.

(2) Key tape segments containing only one key per segment will be destroyed within 12 hours at the end of the cryptoperiod (for example, daily supersession (31 segments)).

7. TRANSPORTING COMSEC KEY

a. Emergency requests for exceptions to use commercial aircraft to transport COMSEC key will be sent to the USAREUR G2 (AEAGB-SAD-S), Unit 29351, APO AE 09014-9351, by the quickest means available. (Figure 1 is a sample request for exception.) The following information must be provided with the request:

(1) COMSEC-key short title, quantity, accounting legend codes (ALCs), CONAUTH, and cryptoequipment to be keyed. The request will be classified no lower than Secret.

(2) Confirmation of CONAUTH notification.

(3) A statement that all other options to meet keying requirements were examined and determined unsuitable (OTAR, local COMSEC accounts, local key generator-83 (KG-83)).

SECRET

DEPARTMENT OF THE ARMY
100TH INFANTRY BRIGADE
UNIT 12345
APO AE 09000-2345

AEAAA-C 1 August 2003

MEMORANDUM FOR USAREUR G2 (AEAGB-SAD-S), Unit 29351, APO AE 09014-9351

SUBJECT: Request for Exception to Policy on Transportation of COMSEC/CCI Material Aboard Non-U.S. Flag Aircraft or Commercial Vehicle (U)

1. (U) References:

a. (U) AR 380-40, Policy for Safeguarding and Controlling Communications Security (COMSEC) Material (para 2-16), 30 June 2000.

b. (U) AE Regulation 380-40, Safeguarding and Controlling Communications Security Material (para 7), 10 July 2003.

2. (S) According to the reference in paragraph 1, request authority to handcarry COMSEC material aboard a non-U.S. flag aircraft from Frankfurt, Germany, to Bucharest, Romania, on or about 10 December 2003. The return flight will be on the same airline on or about 17 December 2003. The mission is in support of a survey and investigation pertaining to recovery of WWII servicemembers buried in Romania.

3. (S) This exception to policy is required to provide secure communications support for the Commanding General, Task Force Eagle, USAREUR Forward, Kaposvar, Hungary, and for the Mission Commander, Bucharest, Romania.

4. (S) Type of Material: 3 Motorola STU-III/A telephones, 1 MFAX secure fax machine, 1 Precision Lightweight GPS Receiver, 1 AKAT A1105, and ALC-1 key. The controlling authority is the U.S. Space Command. The keying material must be loaded on the GPS receiver for precise positioning service. This will be essential to accurately plot the burial sites of the U.S. servicemembers. All other options to meet keying requirements were examined and determined unsuitable. The COMSEC custodian will load the key into the GPS receiver before the time of travel.

5. (S) COMSEC/CCI material will be in the possession of the authorized unit courier at all times. There are no U.S. military flights to Romania during the time of the stated mission.

6. (U) POC is Mr. Smart, DSN 484-2222.

BERNARD F. HILL
Colonel, IN
Commanding

Derived From: AR 380-40, AE Regulation 380-40, EO 12958 I.5c.
Declassify on: (dated) 10 years from date of memo.

SECRET

Figure 1. Sample Request for Exception to Transport COMSEC/CCI Material Aboard Non-U.S. Flag Aircraft or Commercial Vehicle*

***NOTE:** The information shown in figure 1 is unclassified. The classification markings are for demonstration purposes only.

(4) Confirmation that two couriers with TS access will accompany the TS key.

(5) Confirmation of compliance with the requirements of subparagraph b below.

b. Commanders will designate unit personnel as official couriers for classified COMSEC material as follows:

(1) Commanders will use DD Form 2501 to appoint official unit couriers to transport classified material outside U.S. military garrisons and field operating sites within the same country according to AR 380-5, chapter 8; and USAREUR Supplement 1. (DD Form 2501 is an accountable form valid 1 year from date of issue.)

(2) Custodians will sign for courier-authorization cards on the AE Form 380-40A provided by their security manager or S2.

c. One-drawer and two-drawer containers approved by the General Services Administration (GSA) may be used to store classified COMEC key in the field and in transporting vehicles if under continuous surveillance. These containers must be securely fastened to the structure (AR 380-5) in fixed facilities (other than an approved class-A vault or vault-type room guarded or protected by alarms during nonoperating hours).

d. Open storage of COMSEC key is prohibited (AR 380-40).

e. Security containers that have been altered will not be used to store classified COMSEC information and classified collateral material (AR 380-5). Security containers altered for TPI may be used to store classified COMSEC. Additional security containers will not be altered.

8. POLICY FOR KOV-14 CARDS IN THE EUROPEAN REGION

a. The KOV-14 FORTEZZA Plus (Krypton) cryptographic card provides all of the security services for secure-voice data supporting DOD advanced digital communications networks. The KOV-14 card is designated Unclassified ALC-1 regardless of the classification of key it contains. Because of this designation the KOV-14 card is accountable through the CMCS by serial number, from inception until it is physically destroyed. The KOV-14 card is programmed with keying material to protect information up to and including TS and sensitive compartmented information (SCI). The KOV-14 card is the only cryptographic card approved for use with STE.

b. The end user must purchase the KOV-14 card from United States Communications-Electronics Command Communications Security Logistic Activity (USACCSLA). The supporting COMSEC custodian will order the key from USACCSLA.

c. The KOV-14 card provides key for telephones with STE cryptographic capability. There are six different possible states of a KOV-14 card:

(1) BLANK card: Does not contain any stored key or CIK.

(2) FILL card: Contains stored key and CIK.

NOTE: A FILL card must not be used solely as a TERMINAL PRIVILEGE AUTHORITY (TPA) or CARRY card. A FILL card may initially be used to create a TPA card, but it must be immediately associated with at least one STE as a USER card (National Security Telecommunication and Information Systems Security Instruction 3030).

(3) USER card: Contains only stored key.

(4) CARRY card: Contains stored CIK.

(5) TPA CARD: Contains set STE security straps. The TPA card must be associated with an STE (see the note under (2) above).

(6) TRAVELING card: Contains stored key, CIK, and associated personal identification number (PIN) for access (effective on the upgrade of version 2.2).

d. The KOV-14 card must be programmed with keying material (STU-III and Secure Data Network System (SDNS) key) at the National Security Agency (NSA) Electronic Key Management System (EKMS) Central Facility (CF). Account personnel usually will not destroy the KOV-14 card, because the card is recoverable and must be returned to the EKMS CF for reuse or destruction. Currently, all KOV-14 cards shipped to COMSEC accounts contain operational key and have a 1-year cryptoperiod starting when the card is programmed. Before the expiration date, the COMSEC custodian must return the KOV-14 cards to EKMS CF for rekeying.

e. The EKMS CF packs and ships the KOV-14 cards to COMSEC accounts in a sealed transparent security container with a visible yellow key tag. While sealed in this container, users must handle and safeguard the KOV-14 cards as classified cryptomaterial at the level of the key that is programmed in the KOV-14 cards even though the card is accounted for as Unclassified. When received from the EKMS CF, the KOV-14 card is referred to as a FILL card. TPI does not apply to TS KOV-14 cards. The COMSEC custodian will be able to determine the classification of the programmed key by inspecting the yellow key tag. If, for any reason, the COMSEC custodian has to return KOV-14 cards to the EKMS CF before the cards are removed from the sealed transparent security container, the custodian must ship the cards through the Defense Courier Service (DCS).

f. Once the KOV-14 FILL card has been associated with an STE, it is referred to as a KOV-14 USER card. Although the KOV-14 card must be handled as sensitive but unclassified (SBU) COMSEC material when it is removed from its associated STE, the KOV-14 card remains ALC-1 accountable. When not in use, the KOV-14 card must be physically protected by retention in the personal possession of the authorized cleared user or stored to prevent the possibility of loss, unauthorized substitution, tampering, or breakage. Personnel must report lost or stolen KOV-14 cards immediately (k and l below).

g. Commanders will designate a responsible individual to be a TPA. The TPA will be responsible for the configuration of the STE security features, the upgrade of the terminal's software, and the inspection of the terminal's physical integrity. Commanders should assign the TPA as low in their organization as possible.

h. COMSEC custodians will hand-receipt KOV-14 cards to an appointed TPA or card privilege authority (CPA) and authorize them to sub-hand-receipt to end users. In some cases, such as in units or directorates with a large volume of STEs, COMSEC custodians may sub-sub-hand-receipt cards to the users in their area of responsibility. This control will reduce the amount of paperwork and accounting required by the COMSEC custodian. The TPA or CPA will inventory KOV-14 cards each quarter. COMSEC custodians are not required to physically inventory each card for the Semiannual Inventory Report (SAIR) or Change of Custodian Inventory Report (CCIR). Instead, the COMSEC custodian will verify the KOV-14 cards on hand by directing the TPA to physically inventory and certify a written inventory list of the KOV-14 cards by serial number using AE Form 380-40D. The TPA will perform this inventory each quarter. The inventory will be called the Quarterly Possession Inventory (QPI).

NOTE: Personnel authorized to use FILL cards will handle and control the FILL cards more stringently than other KOV-14 cards.

i. Personnel using an STE with a KOV-14 card inserted will consider the STE classified and protect it according to the level of information being processed. To prevent unauthorized use, the user will not leave an STE unattended with a KOV-14 card inserted unless the STE is operated in a sensitive compartmented information facility (SCIF) or other secure environment.

j. When KOV-14 cards are to be transported or shipped, COMSEC custodians will not pack them in the same container with their associated STE. When using commercial carriers, COMSEC custodians will ship KOV-14 cards by separate carrier or mode from that used to ship the associated STE. If the same commercial carrier must be used because of urgent operational requirements, COMSEC custodians will ship KOV-14 cards on a different day from their associated STE.

k. The following occurrences are reportable COMSEC incidents that must be reported within 24 hours (AR 380-40, chap 7):

(1) The loss of a KOV-14 FILL card.

(2) Inconsistencies between the keying material on the cards and information on key tags (for example, mismatch, keying information can be verified after STE association).

(3) Known or suspected tampering of the KOV-14 cards.

(4) Loss of a KOV-14 USER card and associated STE.

(5) Loss of a KOV-14 USER card and an associated KOV-14 CARRY card containing the other half of the KOV-14 USER card key split.

(6) Loss of a TRAVELING card with its written PIN (for example, the PIN written on a sheet of paper that is placed in the card's carry pouch with the TRAVELING card).

l. Reportable administrative incidents include damage to or destruction, loss, or theft of a KOV-14 USER card.

(1) When a reportable administrative incident occurs, the hand-receipt holder must immediately report it to the COMSEC custodian.

(2) The COMSEC custodian will notify NSA, EKMS CF, USACCSLA, Army COMSEC Central Office of Record Tier 1, and HQ USAREUR/7A (AEAGB-SAD-S), using memorandum, e-mail, or electronic message. Administrative incidents are not considered reportable COMSEC incidents as defined in AR 380-40. On receipt of notification, the USACCSLA will remove the card from the COMSEC custodian's assets and NSA will add the key to their compromised key list.

(3) Because the KOV-14 card is purchased using Operation and Maintenance, Army, funds through the Standard Logistic Supply System, commanders will consider appropriate action in response to reportable administrative incidents. Commanders will act according to AR 735-5, chapter 12, with respect to administrative methods to obtain relief from responsibility in accounting for Government property (for example, cash collection, statement of charges).

m. The KOV-14 card is reusable after it has been zeroized. When zeroized, the card is stripped of all user CIK functions. COMSEC custodians will zeroize KOV-14 USER cards using the STE before they ship the KOV-14 cards to EKMS CF for reprogramming, or to a designated vendor for replacement and service. If a KOV-14 card becomes unserviceable and is out of warranty, COMSEC custodians will ship the KOV-14 card as directed by USACCSLA for disposal. COMSEC custodians will send SF 153 with these shipments.

n. Original vendors or authorized persons will service STE and KOV-14 BLANK, USER, and CARRY cards. KOV-14 FILL cards must be serviced by EKMS CF (shipped by DCS).

NOTE: The STE is not a CCI. COMSEC custodians do not account for CCI. The STE is handled and accounted for under the standard logistic supply policy. The STE has tamper seals. The TPA will inspect these seals according to local logistic (PBO) policy. If tampering of an STE is suspected, the TPA will not permit the STE to be placed in operation. Tampering is not a reportable COMSEC incident, but suspected tampering will be reported to the G2 (AEAGB-SAD-S). The TPA will observe and inspect the STE whenever a KOV-14 card is inserted.

9. PROCEDURES FOR DISPOSITION OF KOV-14 CARDS

a. Excess serviceable KOV-14 cards will be re-distributed within field commands and organizations to the extent possible and consistent with operational requirements. Serviceable cards determined to exceed anticipated operational requirements will be reported to the Theater COMSEC Manager (USAREUR G6) for redistribution within the theater.

b. KOV-14 cards may be transferred from COMSEC accounts to the NSA CF for programming or rekey using SF 153 by any of the means identified in (1) through (3) below using the addresses as shown. A key-order request must accompany the SF 153.

(1) DCS Courier: 880111-BA05, EKMS Central Facility, Finksburg, MD 21048-1630.

(2) USPS Registered Mail: National Security Agency, EKMS Central Facility, P.O. Box 718, Finksburg, MD 21048-0718.

(3) Approved commercial carrier: National Security Agency, EKMS Central Facility, 2021 Suffolk Road, Finksburg, MD 21048-1630.

c. When the CF determines that a KOV-14 card received for re-key is defective and cannot be programmed or re-keyed, the CF will take the following actions:

(1) If the card is still under warranty, NSA will provide a new KOV-14 card (free issue) to the user from its existing inventory and obtain a replacement for the defective card for re-stock from the manufacturer. The defective card will be disposed of by the CF.

(2) If the defective card is no longer under warranty, the user COMSEC account will be notified that the card is defective and no longer usable. The CF will automatically transfer the defective card directly to the NSA destruction facility at Fort Meade without any further action by the user.

NOTE: Replacement card acquisition and funding is a user responsibility. Contact the USACCSLA Inventory Manager for instructions on how to procure new KOV-14 cards, (520) 538-8338/DSN 879-8338/7515. Key-order requests for new cards must not be sent directly to the CF.

10. COORDINATION AND APPROVAL OF EMERGENCY PLANS

a. The COMSEC custodian will prepare an emergency plan according to AR 190-13, TB 380-41, UR 190-13, and this regulation. A sample emergency plan is in AE Pamphlet 380-40, appendix D.

(1) The custodian will incorporate the emergency plan into the installation physical security plan.

(2) Commanders will review plans after coordination with appropriate staff agencies. Commanders will approve plans if the plans meet all requirements.

(3) The custodian will list organizations that must be notified during an emergency.

b. An official who is in the rank of at least captain (03) or in the grade of at least GS-12 will decide if armed guards are needed during an emergency. Guards must be trained as prescribed by AR 190-14.

11. COMMAND COMSEC INSPECTIONS

Each COMSEC account will receive a command COMSEC inspection (AR 380-40). Inspections will include a review of unit property book CCI records. A command COMSEC inspector will be appointed at appropriate echelons to conduct these inspections. The inspector will send a report for each inspection to the USAREUR G2 (AEAGB-SAD-S), Unit 29351, APO AE 09014-9351.

12. COMSEC-INCIDENT REPORTING

a. COMSEC-incident reports will be made by electronic message. A sample COMSEC/CCI incident report is in AE Pamphlet 380-40, appendix I.

b. Automatic digital network (AUTODIN) message addressees with Defense Message System (DMS) equivalents (f below) for the European region COMSEC incidents reports (AR 380-40, para 7-3a) are as follows:

(1) Physical Incidents.

(a) Key at the user level:

ACTION ADDRESSEES:
CONAUTH
DIRUSACCSLA FT HUACHUCA AZ//SELCL-SAS-IN//
INFO:
HIGHER HQ AS DIRECTED BY UNIT STANDING OPERATING PROCEDURE (SOP)
DIRNSA FORT GEORGE G MEADE MD//I413//
DIRUSACCSLA FT HUACHUCA AZ//SELCL-ID-OR/SELCL-ID-KEY//
HQ USEUCOM VAIHINGEN GE//ECJ6-I//
CDRUSAREUR HEIDELBERG GE//AEAIM-C4IT-CS/AEAGB-SAD-S//
CDRUSAREUR DCSINT HEIDELBERG GE//
USAREUR PROVOST MARSHAL MANNHEIM GE//AEAPM-PS//
CDR66THMIGP DARMSTADT GE//IAPG-SA/IAPG-SAS//
NCEUR VAIHINGEN GE//F262//
CDR5THSIGCMD MANNHEIM GE//AFSE-IS//
USATCMOEUR11THSIGDET MANNHEIM GE//AFSE-CLC-CMO/5BE001//

(b) Key in distribution channels:

ACTION ADDRESSEES:
DIRNSA FOTT GEORGE G MEADE MD//I413//
DIRUSACCSLA FT HUACHUCA AZ//SELCLSAS-IN//
INFO:
HIGHER HQ AS DIRECTED BY UNIT SOP

CONAUTH
DIRUSACCSLA FT HUACHUCA AZ//SELCL-IN-OR/SELCL-IN-KEY//
HQ USEUCOM VAIHINGEN GE//ECJ6-I//
CDRUSAREUR HEIDELBERG GE//AEAIM-C4IT-CS/AEAGB-SAD-S//
CDRUSAREUR DCSINT HEIDELBERG GE//
USAREUR PROVOST MARSHAL MANNHEIM GE//AEAPM-PS//
CDR66THMIGP DARMSTADT GE//IAGP-SA/IAPG-SAS//
NCEUR VAIHINGEN GE//F262//
CDR5THSIGCMD MANNHEIM GE//AFSE-IS//
USATCMOEUR11THSIGDET MANNHEIM GE//AFSE-CLC-CMO/5BE001//

(c) Key incidents at the CONAUTH level:

ACTION ADDRESSEE:
DIRUSACCSLA FT HUACHUCA AZ//SELCL-SAS-IN//
INFO:
HIGHER HQ AS DIRECTED BY UNIT SOP
DIRNSA FORT GEORGE G MEADE MD//I413//
DIRUSACCSLA FT HUACHUCA AZ//SELCL-ID-OR/SELCL-ID-KEY//
HQ USEUCOM VAIHINGEN GE//ECJ6-I//
CDRUSAREUR HEIDELBERG GE//AEAIM-C4IT-CS/AEAGB-SAD-S//
CDRUSAREUR DCSINT HEIDELBERG GE//
CDR66THMIGP DARMSTADT GE//IAPG-SA/IAPG-SAS//
NCEUR VAIHINGEN GE//F262//
CDR5THSIGCMD MANNHEIM GE//AFSE-IS//
USATCMOEUR11THSIGDET MANNHEIM GE//AFSE-CLC-CMO/5BE001//

(d) Classified COMSEC equipment and documents:

ACTION ADDRESSEES:
DIRNSA FORT GEORGE G MEADE MD//I413//
DIRUSACCSLA FT HUACHUCA AZ//SELCL-SAS-IN//
INFO:
HIGHER HQ AS DIRECTED BY UNIT SOP
CONAUTH
DIRUSACCSLA FT HUACHUCA AZ//SELCL-ID-OR/SELCL-ID-KEY//
DIRUSACCSLA FT HUACHUCA AZ//SELCL-IA-A/SELCL-IA-B//
HQ USEUCOM VAIHINGEN GE//ECJ6-I//
CDRUSAREUR HEIDELBERG GE//AEAIM-C4IT-CS/AEAGB-SAD-S//
CDRUSAREUR DCSINT HEIDELBERG GE//
USAREUR PROVOST MARSHAL MANNHEIM GE//AEAPM-PS//
CDR66THMIGP DARMSTADT GE//IAPG-SA/IAPG-SAS//
NCEUR VAIHINGEN GE//F262//
CDR5THSIGCMD MANNHEIM GE//AFSE-IS//
USATCMOEUR11THSIGDET MANNHEIM GE//AFSE-CLC-CMO/5BE001//

(2) Cryptographic Incidents.

ACTION ADDRESSEES:
DIRNSA FORT GEORGE G MEADE MD//I413//
DIRUSACCSLA FT HUACHUCA AZ//SELCL-ID-SAS-IN//
INFO:
CONAUTH
DIRUSACCSLA FT HUACHUCA AZ//SELCL-ID-OR/SELCL-ID-KEY//
HQ USEUCOM VAIHINGEN GE//ECJ6-I//
CDRUSAREUR HEIDELBERG GE//AEAIM-C4IT-CS/AEAGB-SAD-S//
CDRUSAREUR DCSINT HEIDELBERG GE//
CDR66THMIGP DARMSTADT GE//IAPG-SA/IAPG-SAS//
NCEUR VAIHINGEN GE//F262//

CDR5THSIGCMD MANNHEIM GE//AFSE-IS//
USATCMOEUR11THSIGDET MANNHEIM GE//AFSE-CLC-CMO/5BE001//
HIGHER HQ AS DIRECTED BY UNIT SOP

(3) Personnel Incidents.

ACTION ADDRESSEES:
DIRUSACCSLA FT HUACHUCA AZ//SELCL-SAS-IN//
DIRNSA FORT GEORGE G MEADE MD//I413//
INFO:
HIGHER HQS AS DIRECTED BY UNIT SOP
CDR66THMIGP DARMSTADT GE//IAPG-SA/IAPG-SAS//
HQ USEUCOM VAIHINGEN GE//ECJ6-I//
CDRUSAREUR HEIDELBERG GE//AEAIM-C4IT-CS/AEAGB-SAD-S//
CDRUSAREUR DCSINT HEIDELBERG GE//
USAREUR PROVOST MARSHAL MANNHEIM GE//AEAPM-PS//
NCEUR VAIHINGEN GE//F262//
USATCMOEUR11THSIGDET MANNHEIM GE//AFSE-CLC-CMO/5BE001//

c. Message addressees for COMSEC incident reports (AR 380-40, para 7-3b) in the European region are as follows:

(1) Incomplete or unauthorized destruction:

ACTION ADDRESSEE:
DIRNSA FORT GEORGE G MEADE MD//I413//
CONAUTH
INFO:
HIGHER HQ AS DIRECTED BY UNIT SOP
HQ USEUCOM VAIHINGEN GE//ECJ6-I//
CDRUSAREUR HEIDELBERG GE//AEAIM-C4IT-CS/AEAGB-SAD-S//
CDRUSAREUR DCSINT HEIDELBERG GE//
CDR66THMIGP DARMSTADT GE//IAPG-SA/IAPG-SAS//
DIRUSACCSLA FT HUACHUCA AZ//SELCL-ID-OR/SELCL-ID-KEY//
NCEUR VAIHINGEN GE//F262//
CDR5THSIGCMD MANNHEIM GE//AFSE-IS//
USATCMOEUR11THSIGDET MANNHEIM GE//AFSE-CLC-CMO/5BE001//

(2) Unauthorized retention of COMSEC material past its supersession, use of unauthorized or locally produced key, unauthorized extension of a cryptoperiod, or use of compromised, superseded, defective, or previously used key:

ACTION ADDRESSEES:
DIRNSA FORT GEORGE G MEADE MD//I413//
CONAUTH
INFO:
HIGHER HQ AS DIRECTED BY UNIT SOP
HQ USEUCOM VAIHINGEN GE//ECJ6-I//
CDRUSAREUR HEIDELBERG GE//AEAIM-C4IT-CS/AEAGB-SAD-S//
CDRUSAREUR DCSINT HEIDELBERG GE//
CDR66THMIGP DARMSTADT GE/IAPG-SA/IAPG-SAS//
DIRUSACCSLA FT HUACHUCA AZ//SELCL-ID-OR/SELCL-ID-KEY//
NCEUR VAIHINGEN GE//F262//
CDR5THSIGCMD MANNHEIM GE//AFSE-IS//
USATCMOEUR11THSIGDET MANNHEIM GE//AFSE-CLC-CMO/5BE001//

(3) Administrative Incidents addressed in AR 380-40, paragraph 7-3d:

ACTION ADDRESSEES:
CONAUTH
INFO:
HIGHER HQ AS DIRECTED BY UNIT SOP

d. CCI incidents (formerly CCI-access discrepancies) in the European region will be reported as follows:

NOTE: The requirement in DA Pamphlet 25-380-2 to report certain CCI incidents to the United States Army Information Systems Command has been rescinded.

(1) CCI users will report CCI incidents to their security manager, accountable officer, or PBO.

(2) On receiving a report of a CCI incident, the security manager, accountable officer, or PBO will--

(a) Prepare a CCI-incident report as prescribed in AE Pamphlet 380-40.

(b) Send the report to the addressees below if the incident concerns unkeyed CCI. (COMSEC custodians will become involved only if the incident involves keyed CCI or equipment that is found on the installation and it cannot be determined that the equipment is keyed.)

ACTION ADDRESSEES:
CDRLOGSA REDSTONE ARSENAL AL//AMXLS-M//
DIRUSACCSLA FT HUACHUCA AZ//SELCL-SAS-IN//
CONAUTH (IF KEY IS INVOLVED)
INFO:
DIRNSA FORT GEORGE G MEADE MD//I413//
DIRUSACCSLA FT HUACHUCA AZ//SELCL-IA-A/SELCL-IA-B//
HIGHER HQ AS DIRECTED BY UNIT SOP
HQ USEUCOM VAIHINGEN GE//ECJ6-I//
CDRUSAREUR HEIDELBERG GE//AEAIM-C4IT-CS/AEAGB-SAD-S//
CDRUSAREUR DCSINT HEIDELBERG GE//
USAREUR PROVOST MARSHAL MANNHEIM GE//AEAPM-PS//
CDR66THMIGP DARMSTADT GE//IAPG-SA/IAPG-SAS//
NCEUR VAIHINGEN GE//F262//
CDR5THSIGCMD MANNHEIM GE//AFSE-IS//
USATCMOEUR11THSIGDET MANNHEIM GE//AFSE-CLC-CMO/5BE001//

e. COMSEC incidents involving positive-controlled (keyed) material will be reported according to CJCSI 3260.01 to HQ USEUCOM VAIHINGEN GE//ECJ36(PMCT)// as an action addressee.

f. DMS addresses for COMSEC/CCI incidents:

DIRUSACCSLA FT HUACHUCA AZ//SELCL-ID-SAS-IN//
ou=CSLA Cmd(s), ou=CSLA, 1=FORT HUACHUCA AZ.1=CONUS(s)
ou=organizations, ou=Army, ou=DoD, o=U.S. Government, c=US

DIRNSA FT GEORGE G MEADE MD
(AUTODIN-only organization)

HQ USECOM VAIHINGEN GE//ECJ6-I//
ou=HQ USECOM(s), 1=EUROPE(s), ou=Organizations, ou=EUCOM, ou=DoD,
o=U.S. Government, c=US

CDRUSAREUR HEIDELBERG GE//AEAIM-C4IT-CS//
ou=USAREUR ODCSIM(s), ou=ODCSIM, ou=USAREUR 7A, 1=EUROPE(s),
ou=Organizations, ou=Army, ou=DoD, o=U.S. Government, c=US

CDRUSAREUR DCSINT HEIDELBERG GE//AEAGB-SAD-S//
ou=USAREUR ODCSINT(s), ou=ODCSINT, ou=USAREUR 7A, 1=EUROPE(s)
ou=Organizations, ou=Army, ou=DoD, o=U.S. Government, c=US

USAREUR PROVOST MARSHAL MANNHEIM GE//AEAPM-PS//
ou=USAREUR OPM(s), ou=OPM, ou=USAREUR 7A, 1=EUROPE(s),
ou=Organizations, ou=Army, ou=DoD, o=U.S. Government, c=US

CDR66THMIGP DARMSTADT GE//IAPG-SA/IAPG-SAS//
ou=CDR66MIGP(s), ou=66THMIGP(s), ou=USAINSCOM, 1=EUROPE(s)
ou=Organizations, ou=Army, ou=DoD, o=U.S. Government, c=US

NCEUR VAIHINGEN GE//F262//
(AUTODIN – only organization

CDR5THSIGCMD MANNHEIM GE//AFSE-IS//
ou=5 SIG CMD DCofS Intelligence(s), ou=5SIG CMD, 1=EUROPE(s),
ou=Organizations, ou=Army, ou=DoD, o=U.S. Government, c-US

USATCMOEUR11THSIGDET MANNHEIM GE
ou=TCLSC-E(s), ou=43 SIG BN(s), ou=5 SIG CMD, 1=EUROPE(s), Organizations,
ou=Army, ou=DoD, o=U.S. Government, c=US
CDR LOGSA REDSTONE ARSENAL AL//AMXLS-M//
ou=LOGSA CDR RSA(s), ou=AMC RSA, 1=REDSTONE ARSENAL AL,
1=CONUS(s), ou=Organizations, ou=Army, ou=DoD, o=U.S. Government, c=US

13. STU-III, STE, AND TIMEPORT 280 GSM-SM (SECURE CELLPHONE) INSTALLATION AND USE IN PRIVATE QUARTERS

a. STU-III. Requests for STU-III installation in private quarters will be made according to appendix B. The request must be signed by the first colonel (O6) in the chain of command. Requests must be for high-level officials who require frequent secure-telephone-voice communication after normal duty hours.

(1) Officials not listed in AE Supplement 1 to AR 25-1, appendix D, must submit requests through command channels to the USAREUR G2 (AEAGB-SAD-S), Unit 29351, APO AE 09014-9351, using the format in this regulation, appendix B, figure B-1.

(2) Officials listed in AE Supplement 1 to AR 25-1 will submit a memorandum to the STU-III Residence Manager (AEAGB-SAD-S), HQ USAREUR/7A, Unit 29351, APO AE 09014-9351, when the STU-III is installed in an authorized residence. This memorandum will state the official's name, position, and residential address. This memorandum will be used to ensure accountability of COMSEC key and CCI in private quarters throughout the European region and to help the COMSEC-incident program manager keep an up-to-date database of STU-IIIs, STE, and Timeport 280 GSM-SMs in private quarters. The security manager and information assurance manager (IAM) are responsible for ensuring the STU-III key and the STU-III instrument are returned to the PBO and COMSEC account (respectively) and for notifying the USAREUR G2 (AEAGB-SAD-S), Unit 29351, APO AE 09014-9351, when officials who have this equipment permanently depart the organization or when the secure telephone is no longer required.

(3) The STU-III may be installed in the private quarters of designated essential personnel for the duration of their service in their specific positions.

(4) If the request is approved, the following standards and conditions must be met:

(a) Audio and physical security precautions must prevent unauthorized access to the STU-III and the CIK and interception of information. The following applies:

1. STU-IIIs in private quarters will not be used as standard telephones.

2. Precautions must meet DA security standards (AR 380-5, paras 6-13 and 7-6c, and DA Pam 25-16 on protecting information (physical and electronic), including oral communications).

3. Requests to certify private quarters for classified discussions (AR 381-14) will be made according to UR 380-85, appendix B.

4. Certification for a STU-III in private quarters will be renewed annually. Security managers will notify the USAREUR G2 (AEAGB-SAD-S), Unit 29351, APO AE 09014-9351, for recertification 30 days before the renewal date.

(b) The requester and the security manager will keep a copy of the approval.

(c) Security managers will notify the USAREUR G2 (AEAGB-SAD-S), Unit 29351, APO AE 09014-9351, when STU-IIIs are no longer needed and provide disposition instructions for turning in the STU-III and CIK.

(d) STU-IIIs in private quarters are only for voice communication. Information discussed on STU-IIIs will be no higher than Secret or its non-U.S. equivalent.

(e) The STU-III will be marked "U.S. GOVERNMENT PROPERTY." A locally prepared, self-adhesive label may be used for this purpose. The label must be attached to the STU-III.

(f) The STU-III user must have the appropriate security clearance and be certified by the local commander as having responsibilities involving national security. The user will sign for the STU-III key on AE Form 380-40B.

(g) The STU-III user will attach an adjusted DD Form 2056 to the STU-III and black-out or cut off the part of the label that states "DO NOT DISCUSS CLASSIFIED INFORMATION."

(h) The CIK will be removed from the STU-III after each use.

(i) The CIK will be controlled by the user or left in the custody of an authorized person. DA security standards for STU-IIIs define "authorized persons" and prescribe STU-III controls.

(j) Users will be familiar with and maintain copies of DA security procedures.

b. STE. Procedures for requesting STE in private quarters are the same as those for requesting a STU-III (a above). If the request is approved, the following additional standards and conditions must be met:

(1) Audio and physical-security precautions must prevent unauthorized access to the STE and to FORTEZZA card (KOV-14) and prevent interception of information.

(2) The STE will be marked "U.S. GOVERNMENT PROPERTY." A locally prepared, self-adhesive label may be used for this purpose. The label must be attached to the STE.

(3) The STE user must have the appropriate security clearance and be certified by the local commander as having responsibilities involving national security. The user will sign for the FORTEZZA card on AE Form 380-40D.

(4) The KOV-14 card must be removed from the STE after each use.

(5) The KOV-14 card must be controlled by the user or left in the custody of an authorized person.

c. Timeport 280 With a GSM-SM (Secure Cellphone). The following standards and conditions must be met:

(1) The secure cellphone must be strictly controlled while in the residence.

(2) The secure cellphone may be keyed only up to the Secret level.

(3) Only authorized persons will be allowed access to a keyed secure cellphone.

(4) To prevent unauthorized use or loss, the secure cellphone must be physically separated when not in use and the GSM-SM PIN must be disabled. The GSM-SM must be in the personal possession or stored in a locked cabinet or drawer in an area separate from the Timeport 280.

(5) The secure cellphone will not used to discuss classified information when uncleared personnel are present.

(6) The room where the secure cellphone is used must have a lockable door. The door must be closed and locked during classified discussions.

(7) Notes may not be taken while conducting a classified discussion.

(8) Unusual incidents involving the residence or loss of the secure cellphone must be reported to the COMSEC custodian, information assurance security officer (IASO) or IAM, and Regional Computer Emergency Team, Europe (RCERT-E) (DSN 380-5232), within 24 hours.

(9) The Timeport 280 and 280i must be turned off and returned to the primary hand-receipt holder or PBO with the GSM-SM when they are no longer required. This must be done before moving from the residence, when the residence will be unoccupied for 2 weeks or longer, or before permanent change of station or expiration term of service. The COMSEC custodian, IASO, or IAM must be notified when the Timeport 280 or 280i and the GSM-SM are returned to the primary hand-receipt holder or PBO.

d. Sectèra Timeport 280 and 280i GSM Cellphone.

(1) Users of the Sectèra Timeport 280 and 280i GSM cellphone will detach the SM from the cellphone and place it in their pocket whenever they enter an area where cellphones are not authorized (for example, SCIF, secure workareas). The cellphone (without the SM) may then be placed in the cellphone receptacle-holding container (box) before entering the area.

(2) The loss of a GSM-SM is a reportable COMSEC incident. It must be reported verbally to the COMSEC custodian within 12 hours. No later than 24 hours after the loss, the user will submit a written, signed statement describing the lost material and the circumstances leading to the loss and send the statement to the primary hand-receipt holder, COMSEC custodian, and PBO. The statement must include the following:

(a) Classification. This will depend on whether or not the statement is classified.

(b) Individual's full name, rank or grade, and social security number.

(c) Unit or activity (including division and branch).

(d) The SM serial number.

(e) Incident description. This would include the date, time, and place of discovery as well as a complete description that would explain who, what, when, where, why, and how the SM was lost.

(f) An explanation of actions taken to locate the SM.

(3) Users of the Timeport 280 and 280i with a GSM-SM will sign a user agreement before using the cellphone (fig 2). Users authorized by AE Supplement 1 to AR 25-1 and the G2 to take the Timeport 280 or 280i with the SM home will sign a residence acknowledgement (fig 3). Users must ensure the SM is detached and stored in a locked drawer away from the cellphone when the user is away from the residence and does not have the cellphone on his or her person.

14. FOREIGN ACCESS

a. Local national (LN) employees will not be granted access to keyed CCI based solely on duties. LN employees of the U.S. Government who are involved in and directly support U.S. Government operations may be granted access to CCI keyed with an unclassified U.S. key. LN employees--

(1) May sign hand-receipts for the U.S. unclassified key.

(2) Are not authorized to sign hand-receipts for any CCI equipment.

(3) Must have an appropriate host-nation security check (UR 604-1) and meet the prerequisites of AR 380-40 to sign for or have access to Unclassified U.S. COMSEC key.

b. LN employees required to maintain telecommunications and automated information systems are not authorized to sign a hand-receipt for CCI equipment. PBOs must be U.S. citizens.

c. The security manager of the supported organization will provide the supporting COMSEC-account custodian a list of LN employees authorized to sign a hand-receipt for unclassified COMSEC key. The list will--

(1) Be maintained on each LN employee listed by the Civilian Personnel Operations Center.

TIMEPORT 280i WITH A GSM-SM USER AGREEMENT

I acknowledge, understand, and will comply with the following instructions on the use of a Timeport 280i with a GSM-SM:

1. The Timeport 280i with GSM-SM will remain in my control at all times.

2. The PIN will not be affixed to the Timeport 280i, GSM-SM, or any carrying cases for these devices. It must be kept in a separate location from the cellphone.

3. The Government-issued Timeport 280i with GSM-SM will be used only for official telephone calls.

4. Only authorized persons will be allowed access to a keyed Timeport 280i with GSM-SM.

5. I will not use the Timeport 280i with GSM-SM to discuss classified information when in public or other places where uncleared personnel are present.

6. Any room where the Timeport 280i with GSM-SM is used must have a lockable door, and that door must be closed and locked during classified discussions.

7. I will not take notes while conducting a classified discussion.

8. If I lose a keyed Timeport 280i, I will report the loss to the primary hand-receipt holder, COMSEC custodian, and PBO immediately (not to exceed 12 hours). Security incidents involving an unkeyed Timeport 280i must be reported to the primary hand-receipt holder, COMSEC custodian, and PBO within 24 hours.

9. I will ensure the Timeport 280i and the GSM-SM are returned to the COMSEC primary hand-receipt holder when I no longer require them.

_____ (Date)

_____ (Signature and Printed Name, Rank, and Title)

Figure 2. Timeport 280i User Agreement

(2) Show whether or not that the employees have had a security check.

(3) State that the employees listed have met the conditions of DA Pamphlet 25-16, paragraph 3-4, and are authorized access to a STU-III.

d. Requests for accreditation for secure subscriber terminals (AR 380-19, chap 4) will state that LN employees will operate the terminal.

e. Keys for terminals with approved foreign access must be ordered to include a foreign-access indicator (such as US/FORN, US/UK). If the terminal is not keyed accordingly, unescorted access by an LN employee is not authorized.

15. RELEASE OF CCI

a. Requests for release of CCI will be made according to DA Pamphlet 25-380-2, paragraph 2-6. Requests will be addressed through the USAREUR G2 (AEAGB-SAD-S), Unit 29351, APO AE 09014-9351, to HQDA (DAMI-CDS), 100 Army Pentagon, WASH DC 20310-1001.

b. Questions about release of CCI in the European region will be directed to the G2 at DSN 370-7214 or e-mail: *rademacj@hq.hqusareur.army.mil*.

16. CRYPTOGRAPHIC ACCESS PROGRAM

a. The security manager will be the DACAP POC. Security mangers will coordinate with the unit COMSEC custodian for a list of personnel who have access to a TS key. The program also pertains to cryptographic maintenance, engineering, or installation technicians, regardless of their clearance, who meet the full maintenance qualifications of AR 25–12 and have access to full maintenance manuals that contain cryptologic. Security managers will brief and terminate personnel according AR 380-40, chapter 8, and maintain a database of enrolled personnel. Security managers will send an updated list of personnel enrolled in DACAP to the European Region DACAP Program Manager (USAREUR G2 (AEAGB-SAD-S), Unit 29351, APO AE 09014-9351), by the 20th of each month. Negative reports are required.

ACKNOWLEDGMENT OF SECURITY PROCEDURES FOR USING A TIMEPORT 280i WITH A GSM-SM IN PRIVATE QUARTERS

I acknowledge, understand, and will comply with the following instructions on the use of a Timeport 280i with a GSM-SM PIN in a residence.

1. The Timeport 280i with a GSM-SM PIN must be in my control at all times while in my residence.

2. The SM PIN must not be written on or otherwise affixed to the Timeport 280i, GSM-SM, or any carrying case for these devices.

3. The Timeport 280i with GSM-SM installed will be keyed only up to the Secret level.

4. The Timeport 280i with GSM-SM installed may be used for unclassified calls.

5. For unclassified use, the user should not be discussing any classified information.

6. Only authorized persons will be allowed access to a keyed Timeport 280i and GSM-SM.

7. The GSM-SM must be in my personal possession or stored in a locked cabinet or drawer in an area separate from the Timeport 280i.

8. I will not use the Timeport 280i with the GSM-SM PIN enabled to discuss classified information when uncleared personnel are present.

9. The room in which the Timeport 280i with an enabled GSM-SM PIN is used will have a lockable door. This door must be closed and locked during classified discussions.

10. I will not take notes while conducting a classified discussion.

11. I will report any unusual incidents involving my residence, loss of the Timeport 280i, on loss of the GSM-SM to the primary hand-receipt holder, COMSEC custodian, and PBO within 24 hours. The COMSEC custodian will contact the IASO or IAM.

12. I will ensure that the Timeport 280i and the GSM-SM are returned to the primary hand-receipt holder when I no longer need them.

_____ (Date)

_____ (Signature and Printed Name, Rank, and Title)

Figure 3. Acknowledgment of Security Procedures Using a Timeport 280i in Private Quarters

b. The following information is required before personnel may be added to the access program:

(1) Name, rank or grade, social security number, security clearance.

(2) Date enrolled in the DACAP and date eligible for return from overseas (DEROS).

(3) Official unit address.

(4) Command, barracks, or casern (as applicable).

(5) City and country.

(6) DACAP POC name, unit, and telephone number.

c. The following information must be sent to the European Region DACAP Program Manager for deletion of personnel from the DACAP:

(1) Name, rank or grade, unit.

(2) Date debriefed.

(3) Confirmation that termination statement was signed.

(4) The reason for leaving the program (for example, permanent change of station, change of duty position, expiration term of service, security clearance revoked, access denied).

APPENDIX A
REFERENCES

SECTION I
PUBLICATIONS

A-1. CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION
Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3260.01, Joint Policy Governing Positive Control Material and Devices

A-2. ARMY REGULATIONS

AR 25-1 with AE Supplement 1, Army Information Management

AR 25-12, Communication Security Equipment Maintenance and Maintenance Training

AR 25-400-2, The Army Records Information Management System (ARIMS)

AR 71-32, Force Development and Documentation–Consolidated Policies

AR 190-13, The Army Physical Security Program

AR 190-14, Carrying of Firearms and Use of Force for Law Enforcement and Security Duties

AR 190-40, Serious Incident Report

AR 190-51, Security of Unclassified Army Property (Sensitive and Nonsensitive)

AR 380-5 with USAREUR Supplement 1, Department of the Army Information Security Program

AR 380-19, Information Systems Security

AR 380-40, Policy for Safeguarding and Controlling Communications Security (COMSEC) Material

AR 381-14, Technical Countermeasures (TCI)

AR 710-2, Inventory Management 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, Policies and Procedures for Property Accountability

A-3. DA PAMPHLETS

DA Pamphlet 25-16, Security Procedures for the Secure Telephone Unit, Third Generation (STU-III)

DA Pamphlet 25-380-2, Security Procedures for Controlled Cryptographic Items

A-4. TECHNICAL BULLETIN
TB 380-41, Procedures for Safeguarding, Accounting, and Supply Control of COMSEC Material

A-5. ARMY IN EUROPE PUBLICATIONS

AE Pamphlet 380-40, Communications Security Custodian Guide

USAREUR Regulation 190-13, The USAREUR Physical Security Program

USAREUR Regulation 190-40, Serious Incident Report

USAREUR Regulation 350-1-2, Policy, Procedures, and Responsibilities for Combined Arms Training Center Courses of Instruction

USAREUR Regulation 380-85, Counterintelligence Services

USAREUR Regulation 604-1, Foreign National Screening Program (Laredo Leader)

A-6. MISCELLANEOUS PUBLICATIONS

National Security Telecommunications and Information Systems Security Instruction 3030, Operational Systems Security Doctrine for the FORTEZZA PLUS (KOV-14) Cryptographic Card and Associated Secure Terminal Equipment (STE)

Electronic Key Management System Key Management Plan 702.01, STU-III Key Management Plan (published by the National Security Agency)

NAG-16, Field Generation and Over-the-Air-Distribution of COMSEC Key in Support of Tactical Operations and Exercises

NAG-53, Keying Standard for Non-Tactical KG-84A/C and KIV-7/7HS 7HSA 7HSB Secured Point to Point Circuits

SECTION II
FORMS

A-7. STANDARD FORMS

SF 153, COMSEC Material Report

SF 700, Security Container Information

SF 702, Security Container Check Sheet

A-8. DD FORMS

DD Form 1348-1A, Issue Release/Receipt Document

DD Form 1348-2, DOD Issue Release/Receipt With Address Label

DD Form 1574, Serviceable Tag – Materiel

DD Form 1577, Unserviceable (Condemned) Tag – Materiel

DD Form 1577-2, Unserviceable (Repairable) Tag – Materiel

DD Form 2056, Telephone Monitoring Notification Decal

DD Form 2501, Courier Authorization Card

A-9. DA FORMS

DA Form 1687, Notice of Delegation of Authority - Receipt for Supplies

DA Form 2028, Recommended Changes to Publications and Blank Forms

DA Form 2407, Maintenance Request

DA Form 2653-R, COMSEC Account - Daily Shift Inventory

DA Form 2765-1, Request for Issue or Turn-In

DA Form 3964, Classified Document Accountability Record

DA Form 5941, COMSEC Material Disposition Record

A-10. AE FORMS

AE Form 380-40A, Accountability Register for DD Form 2501 (Courier Authorization)

AE Form 380-40B, COMSEC Custodian STU-III-Key Accountability Record

AE Form 380-40C, Electronic Key Management (EKM) Worksheet

AE Form 380-40D, KOV-14 Card Control Roster and Quarterly Possession Inventory

AE Form 380-40E, Sectèra Secure GSM Worksheet

APPENDIX B
STU-III PROGRAM GUIDANCE

B-1. PURPOSE
This appendix provides guidance for personnel in the European region involved in the STU-III program.

B-2. REGISTRATION

a. The Army in Europe Electronic Key Management System (EKMS) release authority requires a certification statement before a user-representative will be registered for Top Secret (TS) or sensitive compartmented information (SCI) key-ordering privileges. A sample certification statement is provided in the STU-III EKMS Key Management Plan 702.01.

(1) For TS key, the unit security manager must certify that the TS key will be used only in an area approved for TS.

(2) The site security officer will sign the SCI key-certification statement on unit letterhead stationery.

(3) Certification statements will not be sent with the key-order request.

b. To register for TS or SCI key-ordering privileges, the requester must have a supporting communications security (COMSEC) account approved for TS. COMSEC-account support may be provided by any organization or command. A copy of the designated supporting COMSEC account's Account Registration Packet must be sent with the request.

B-3. MANAGEMENT

a. Although the National Security Agency (NSA) program stresses the use of a seed key, an operational key may be required. The type of key to order will be based on specific requirements.

b. The key will be signed for, stored, issued, reported, and handled according to AR 380-40, DA Pamphlet 25-16, STU-III EKMS Plan 702.01, and other COMSEC accounting directives.

c. Each office, unit, organization, and command must establish local policy for cryptoignition keys (CIKs). CIKs must be handled, controlled, inventoried, and managed according to key-control directives.

d. To turn in a defective STU-III, the user must prepare the documentation for turn-in of a defective STU-III and use the checklist at the back of the STU-III operators manual to identify the problem. The user must identify the checklist item by number and give a short explanation of the problem. Appendix C provides controlled cryptographic item (CCI) turn-in procedures.

e. Unused STU-III key storage device (KSD) 64As that have expired will be returned to the COMSEC custodian. A destruction report will be sent to the EKMS Central Facility (CF). If there is no way to destroy the key, the key may be transferred to the EKMS CF. Custodians will use SF 153 to dispose of keys.

NOTE: A destruction report requires two signatures unless it is a consolidated destruction report.

f. Users will zeroize the STU-III three times before turning it in to the supply system. STU-IIIs that cannot be zeroized must be handled as classified material at the classification level of the key.

g. When a STU-III is turned in to the supply system, the instrument should be complete (that is, the operator manual, one blank CIK, line cord, power supply, and all other original issue accessories). Appendix C provides CCI turn-in procedures.

h. Once keyed, the STU-III key is valid for 1 year. The message "CALL KMC" means the key is about to expire. To rekey, users in Germany may call the rekey number at 118. If this does not work or if it is busy, users with "99" (civilian) access in Germany may call the toll-free rekey number at 99-0800-810-7520. Users with worldwide DSN access may call 312-550-STU3 (7883) or 312-936-1810. Users with worldwide commercial access may call 001-410-526-3200. Users should set a deadline for rekeying each STU-III before the annual expiration date. Quarterly rekey is recommended because it is more cost effective.

i. When deploying, a STU-III will not be zeroized. The STU-III will be transported as sensitive material. The CIK will be removed and carried separately.

j. To prevent security violations, STU-III terminals display information to identify the contacted STU-III terminal, the maximum classification level for calls, SCI authorization, and, if other-than-U.S.-access only, foreign access to the terminal (for example, US/UK, US/FORN).

B-4. REPORTS

a. Key destruction reports will include a single signature and the serial number for the STU-III. If an SF 153 is used, the serial number goes in the remarks column across from the appropriate key.

(1) Certified consolidated destruction reports will not include the STU-III serial number, but may be submitted based on a document with a single signature and serial number to the EKMS CF.

(2) Any form (for example, SF 153, DA Form 3964) may be used to record the destruction of a STU-III key if the form--

(a) Clearly identifies the key by its short title, edition, and register number.

(b) Shows signatures and the STU-III serial number. Signatures of the destruction official and a witness are required to authenticate a report of destruction if the STU-III serial number is not used, the key is zeroized, or the key failed to properly load the telephone.

b. A lost CIK is not a COMSEC incident if it is reported to the local security manager within 72 hours. A lost CIK will not be reported to the COMSEC Material Control System (CMCS) EKMS CF unless the associated STU-III is missing.

c. Missing STU-IIIs must be reported to the security manager and unit property book officer (PBO). Missing STU-IIIs must be investigated according to AR 380-5 and DA Pamphlet 25-380-2.

B-5. FORMAT FOR REQUESTING A STU-III FOR PRIVATE QUARTERS

Requests to install a STU-III in private quarters will be prepared using the format in figure B-1.

B-6. SECURITY STANDARDS AND PROCEDURES FOR SECURE CELLPHONES IN VEHICLES

a. The security and integrity of any secure cellphone installed in vehicles must meet the following standards:

(1) The unkeyed secure cellphone is a CCI and will be treated as a sensitive, high-value item and safeguarded according to AR 190-51, AR 380-5, AR 380-40, AR 710-2, DA Pamphlet 25-16, and DA Pamphlet 25-380-2. When mounted in the vehicle and unattended, the secure cellphone must have double-barrier protection (a locked vehicle in a secure or locked facility) (AR 190-51).

(2) Secure cellphone access will be limited to authorized persons. Access to the area where the cellphone is located may be granted to unauthorized persons (without the constant presence of an authorized person) when the following conditions are met:

(a) Access is required by custodial duties or other operational responsibilities.

(b) The area in which the instrument will be used is a controlled U.S. facility.

(c) The CIK is in the personal possession or custody of an authorized person or stored as described in (8) below.

(3) Audio precautions are taken to prevent unauthorized interception of information being discussed over a secure cellphone.

(4) The secure cellphone is used only for voice communication, and the classification of information discussed is no higher than the approved classification level.

(5) The secure cellphone is marked “U.S. GOVERNMENT PROPERTY.”

(6) A label is on the secure cellphone with the following statement: “THIS TELEPHONE IS SUBJECT TO MONITORING AT ALL TIMES. USE OF THIS TELEPHONE CONSTITUTES CONSENT TO MONITORING.”

DEPARTMENT OF THE ARMY
REQUESTER'S UNIT
UNIT 12345
APO AE 00000-2345

AEAQQ-IS-S 1 August 2003

MEMORANDUM FOR USAREUR G2 (AEAGB-SAD-S), Unit 29351, APO AE 09014-9351

SUBJECT: Request for STU-III, STE, Timeport 280 GSM-SM (Secure Cellphone) Installation and Use in Private Quarters

1. References:

a. AR 381-14, Technical Counterintelligence (TCI), 30 September 2002.

b. AE Regulation 380-40, Safeguarding and Controlling Communications Security Material, 10 July 2003.

2. Request approval for installation of a secure telephone in the private quarters of COL John M. Smith, Commander, 2d Brigade, 1st Armored Division. COL Smith's quarters do not qualify for technical surveillance countermeasure support as defined in AR 381-14.

3. The STU-III is required in COL Smith's quarters for secure voice communications according to AR 380-19, chapter 4. COL Smith must be able to initiate and receive secure communications at home after normal duty hours to make time-sensitive decisions based on classified or sensitive information. Without a secure telephone in his quarters, he must drive to the casern (approximately 8 kilometers away) to place or receive secure communications. This delay in response time could adversely affect the unit mission when these communications involve contingency-operation support.

4. The STU-III will be installed at Flieger Str. 58, Sherman Circle, George Washington Village, 67657 Kaiserslautern. The STU-III will be located in an area that will prevent normal voice-level conversations from being overheard by unauthorized persons in or outside the residence.

5. Headquarters, 1st Armored Division, will provide logistic support for the (DSN or Deutsche Telekom) telephone line. DD Form 2056 (Telephone Monitoring Notification Decal), with the top portion of the decal blacked out, will be attached to the STU-III.

6. The security manager for this STU-III is Mr. Smart at DSN 490-XXXX. Maintenance and trouble support will be provided by CW3 Jones at DSN 490-XXXX, civilian 0671-609-XXXX, after duty hours.

7. The security standards and conditions as cited in reference 1b have been met. The STU-III is keyed with Secret, residence only, voice key. *The requester must enter one of the following statements:*

a. The residence is cleared for storage of classified material. The residence has a General Services Administration (GSA) approved, one-drawer storage container.

b. Classified information will not be stored at the residence.

8. The POC for this request is Mr. Smart, DSN 490-XXXX.

FOR THE COMMANDER:

MICHAEL G. ROGERS
Colonel, GS
Chief of Staff

Figure B-1. Sample Request for a STU-III in Private Quarters

(7) If the secure cellphone has been keyed (that is, a CIK has been inserted), the cellphone is cleared for the classification level of the key. Using a keyed secure cellphone is equivalent to openly displaying a classified document. A keyed secure cellphone should never be left unattended.

(8) The CIK must be removed from the secure cellphone after each use. The CIK will remain with the authorized user or stored in an authorized security container.

(9) The CIK will be controlled by the user. If an individual in the area is not cleared to the level of the keyed terminal, the terminal must be under the operational control of an authorized person.

b. The user of a secure cellphone in a vehicle must be thoroughly familiar with the security provisions in subparagraph a above. Questions and problems may be referred to the supporting security manager.

B-7. STU-III USE IN NON-NATO COUNTRIES

STU-IIIs are not ordinarily required when participating with non-NATO countries during joint training if U.S.-to-U.S. secure communications are not needed. The commander will decide whether or not a STU-III will be needed during joint activities with non-NATO countries. (STU-IIIs will not be taken to non-NATO countries unless their use is fully justified.)

a. If a STU-III is needed, the commander will conduct a risk assessment before taking the STU-III into the non-NATO country. This risk assessment will confirm--

(1) Knowledge of and ability to comply with security provisions of DA Pamphlet 25-16 and DA Pamphlet 25-380-2 (including shipping, control, and storage of and access to STU-IIIs in non-NATO countries).

(2) Host-nation approval. Use of a STU-III without host-nation approval is illegal. STU-IIIs can disrupt local telephone systems and be confiscated by post-telephone-telegraph authorities.

(3) An agreement or arrangement has been or can be made to ensure that STU-IIIs will not be seized by customs officials for examination or as illegal devices.

(4) Suitable provisions have been made for securing the CIK.

b. In the risk assessment, the commander will consider that--

(1) Non-NATO countries do not have status-of-forces agreements with the U.S. military. Laws in non-NATO countries may be more restrictive than those of NATO countries. Full compliance with local laws is required.

(2) While the host-country clearance can be avoided by sending the STU-III in a diplomatic pouch, it will not prevent host-country authorities from confiscating the STU-III if it is a “prohibited or unauthorized item” or if it is subsequently used illegally (without host-country approval).

(3) Joint activities are intended to promote mutual trust and further military cooperation. Because CCI security procedures prohibit countries from sharing the STU-III, having a STU-III could be perceived by the host country as a lack of trust.

(4) Local telephone systems may not permit direct contact to the key management center (KMC).

(5) Taking a keyed STU-III avoids the need to call the KMC. If the STU-III is taken keyed, the STU-III and CIK must be stored separately.

(6) Alternative secure communications exist (for example, using a KL-43 or secure systems at a U.S. embassy).

APPENDIX C
SECURITY OF CONTROLLED CRYPTOGRAPHIC ITEMS

C-1. PURPOSE
This appendix provides security policy for controlled cryptographic items (CCIs) in the European region.

C-2. PROTECTIVE MEASURES
The physical security measures described below establish minimum standards for controlling access to CCIs (installed or uninstalled) to protect against tampering, loss, and unauthorized use.

a. Personnel responsible for providing physical protection for unattended CCIs (for example, CCIs not under continuous surveillance by a U.S. citizen permanently assigned to the activity) will--

(1) Store unattended or unkeyed CCI equipment in a zeroized condition.

(2) Store unattached CCIs in a room or building where the doors, windows, and other means of entry and exit can be locked or secured. Physical access must be controlled according to "double-barrier protection" as prescribed in AR 190-51, paragraph 3-24c. The first barrier is the lockable room or building. The second barrier may be a lockable closet, a steel wall locker, steel cage, steel-chain or cable-lock assemblies, lockable steel filing cabinet, or similar barriers.

(3) Secure CCIs directly to tactical vehicles (enclosed van (shelter), trailer, armored vehicle, or aircraft) using U.S. Government-approved series-200 high-security padlocks.

(a) Attach the CCI with an appropriate length of U.S. Government-approved hardened steel chain. Use ⅜-inch trade-size, tool-resistant, case-hardened security chain or ⅜-inch trade-size, grade 80-alloy steel chain conforming to Federal Specification RR-C-271.

(b) Park and protect aircraft and vehicles containing CCIs as indicated in AR 190-51, paragraph 3-24. This method is preferred for operational readiness. Dismounting and remounting CCIs in vehicles and aircraft tends to increase damage to connectors, cabling, knobs, switches, and dials.

(4) Post a sign stating "OFF LIMITS TO UNAUTHORIZED PERSONNEL" at CCI activity entrances (including buildings and motorpools (AR 190-51, para 3-24c(4))). Signs should be posted on wall lockers, cages, or any other CCI storage facilities.

b. Physical protection for attended (unkeyed or keyed) CCIs will be provided as follows:

(1) Unkeyed CCIs must be under the continuous control of an authorized individual permanently assigned to the activity. No additional physical protective measures are required.

(2) Keyed CCIs being used or ready for use will be protected as follows:

(a) A person appropriately cleared for the classification level of the key in the device must keep the keyed CCI under continuous surveillance.

(b) Responsible personnel must increase area controls to match the protection criteria for the classification involved.

(c) When CCI FILL devices (AN/CYZ-10, KYK-13, KOKs) are loaded with classified key, responsible personnel will store them to meet the same requirement as the key-classification-storage requirements. Secret FILLS must be stored in a General Services Administration (GSA)-approved security container; Top Secret FILLS must be stored in a GSA-approved security container with a built-in X-07 lock, under two-person integrity (TPI).

(d) Where fulltime-operated or parttime-manned circuits terminate in spaces that are not authorized for open storage of information classified at or above the level of the traffic encryption key (TEK) used, the circuit must be deactivated when appropriately-cleared persons are not present in both terminal spaces. For KIV-7 secured terminals, circuit deactivation may be accomplished by removing and securing the cryptoignition keys (CIKs); for the KG-84 secured terminals, circuit deactivation requires zeroizing the TEK (NAG 53).

c. CCI and other unclassified communications security (COMSEC) hardware items will be entered into the Standard Army Supply System and logistically managed under AR 710-2, AR 725-50, and DA Pamphlet 25-380-2 (AR 380-40, para 2-3b(2)). Property book officers (PBOs) who use retail stock record accounts will account for unclassified COMSEC equipment using the Standard Logistics System (AR 710-2, para 1-18d(2)). This category of COMSEC material includes equipment and secondary items designated as CCI. CCIs are identified in the FEDLOG with a controlled item inventory code (CIIC) of 9.

(1) Current Army policy (AR 710-2 and DA Pam 25-380-2) requires accounting for CCIs using the Standard Logistic System. Sometimes equipment manufacturers, contractors, or other services will ship CCIs to the wrong Army COMSEC account. To maintain an accurate audit trail for this sensitive material, the COMSEC custodian must follow the procedures for the receipt and transfer of COMSEC material (TB 380-41) as follows:

(a) COMSEC custodians will sign a receipt for the material, post it to their COMSEC accounting records to establish an audit trail, return a signed receipt (SF 153) to the shipper, and send a copy to the Army COMSEC Central Office of Record.

(b) The custodian will immediately coordinate with the PBO and make a transfer to the unit property book. To meet the accounting requirements of AR 380-40 and AR 710-2, an SF 153 will be used as a transfer document between the property book account and the COMSEC account. The PBO may use this form as a voucher and post it to his or her accounting records as with any other receipt.

(2) The PBO is required to take specific actions when CCI equipment is delivered through official distribution channels, contractors, or other HQDA equipment-fielding programs and the equipment is not currently authorized on the unit modification table of organizations and equipment or tables of distribution and allowances. When this type of delivery occurs, the PBO must initiate action through command or operational channels to validate and confirm the continued need for the equipment. The PBO will not refuse to accept transfers or refuse to receipt and account for CCIs from the COMSEC account on property book records. The PBO will accept the equipment regardless of authorization under Vertical--The Army Authorization Documents System (VTAADS). The establishment of such authorization for equipment automatically distributed to units and organizations is a separate administrative management action that must be initiated according to AR 71-32.

(3) When a CCI is shipped or transferred directly to a property book account and the CCI has not been processed by the installation accountable officer, the CCI must be reported to the installation supply support activity (SSA). This reporting will be done according to AR 710-2, paragraph 2-8, and will be in addition to reporting under the Unique Item Tracking (UIT) Program according to AR 710-3.

(4) Certain Army elements performing classified or sensitive operational or test missions and other support functions may require CCIs to be controlled by a COMSEC account to prevent mission disclosure or for other valid reasons. COMSEC custodians will document these situations and send requests for waivers to Army CCI accounting policy through command channels to HQDA (DAMI-CDS) for approval.

C-3. PROCEDURAL MEASURES

a. CCIs for units in the European region will be shipped by U.S. registered mail to the supporting class 7 SSA. The SSA will--

(1) Provide physical security appropriate for high-value sensitive items when the CCI arrives.

(2) Immediately notify the unit that its CCI is ready for pick up.

(3) Continue to notify the unit for 30 days. If the unit does not pick up the CCI within 30 days, the SSA will send a record-of-notification attempts through command channels to the unit.

b. Personnel will annotate DA Form 2653-R for keyed CCIs stored in a GSA-approved security container whenever the container is opened. (DA Form 2653-R entries do not apply to a COMSEC material direct support activity (CMDSA).)

c. Authorized personnel will inventory keyed CCI according to TB 380-41, paragraph 4-15c. These personnel will annotate DA Form 2653-R with the date and initials of the person conducting the inventory before closing and locking the container.

d. Commanders will ensure the following security measures are used:

(1) Access to the facility or area will be controlled according to AR 190-51 and DA Pamphlet 25-380-2. Physical access will be limited to authorized individuals.

(2) Access to keys and locks protecting the CCI will be controlled according to AR 190-51, appendix D.

(3) Periodic command-directed inventories and quarterly sensitive-item inventories will be conducted according to AR 710-2.

(4) The facility, vehicle parking area, and aircraft parking apron where CCIs are located will be checked by guards or other duty personnel. Checks will be made and recorded at least twice during each watch or shift.

(5) As a minimum, the activity standing operating procedure (SOP) will include instructions for safeguarding CCI, controlling access, and reporting CCI incidents (AR 190-51, para 3-24).

C-4. CCI INCIDENTS
Security managers, COMSEC custodians, and PBOs should be familiar with the procedures to report and investigate CCI incidents in TB 380-41, chapter 5; this regulation; and AE Pamphlet 380-40.

a. Reporting Incidents. Security managers, COMSEC custodians, and PBOs will initially report available information. Additional information will be added to interim or final reports to help system evaluators make damage assessments.

NOTE: Corrective action must be included in the last paragraph of final incident messages.

(1) CCI incidents involving unkeyed CCI material will be reported through official channels as follows:

(a) COMSEC channels according to this regulation and TB 380-41.

(b) Logistic channels according to AR 710-3, section V.

(c) Operation channels according to AR 190-40 and UR 190-40.

(2) Incidents involving keyed CCI equipment are COMSEC incidents. CCI incidents must be reported by the COMSEC custodian according to AR 380-40, this regulation, and AE Pamphlet 380-40. Keyed CCI (COMSEC incidents) must be reported through logistic channels, according to AR 710-3, section V, and through operational channels according to AR 190-40 and UR 190-40.

(3) COMSEC custodians will classify CCI initial incident reports Confidential and submit them within 36 hours after the incident is discovered. Interim or final incident reports may be unclassified.

(4) The unit security manager will report CCI equipment involved in a theft of a military vehicle or black market activity as a category 3 serious incident report (SIR). The unit security manager will send the SIR to the local base support battalion provost marshal's office according to AR 190-40 and UR 190-40. The provost marshal will report to higher headquarters as necessary.

b. Investigating Incidents.

(1) The commander will appoint an investigating officer to conduct a preliminary inquiry to determine the facts and circumstances surrounding the incident according to AR 380-5.

(2) The preliminary inquiry will be completed by the investigating officer and forwarded through the USAREUR G2 (AEAGB-SAD-S), Unit 29351, APO AE 09014-9351, to the United States Army Communications-Electronics Command Communications Security Logistic Activity (USACCSLA) (SELCL-ID-SAS-IN), Fort Huachuca, AZ 85613-7090, within 10 duty days after the date of appointment.

(3) The commander will initiate a report of survey according to AR 735-5 if the preliminary inquiry finds negligence was involved in the loss of CCI.

(4) The PBO will originate a UIT report within 24 hours after notification of a loss of CCI (AR 710-3).

c. Routing of CCI Incident Reports. This regulation, paragraph 12, lists the required action and information plain language addresses (PLAs) for CCI incident reports. AE Pamphlet 380-40, appendix I, shows a sample CCI incident message.

C-5. CCI EMERGENCY PLANNING
DA Pamphlet 25-380-2, paragraph 2-11, prescribes the basic requirements for CCI emergency planning.

a. Personnel assigned to an activity using COMSEC material must be familiar with their duties and responsibilities in executing the CCI emergency plan.

b. Commanders will conduct a quarterly practice drill of various portions of the emergency plan. Commanders will document and keep a record of the practice drills on file with the emergency plan.

C-6. TRANSPORTATION OF CCI
Transportation methods must provide the protective measures and security necessary to prevent or deter unauthorized access to CCI. A signature record of persons having accountability and custody from pick-up point to drop-off point must be kept. Commanders will not grant a non-U.S. citizen access to CCIs based solely on the duties of the individual. Commanders will not place CCIs in the custody or control of a non-U.S. citizen (this reg, para 14). Commanders may use one or a combination of the following to transport CCIs:

a. An Officially Certified CCI Courier. If the CCI must be transported using a courier, the courier will be briefed on his or her duties and responsibilities by the courier's security manager. The courier will sign a CCI courier certification memorandum (fig C-1) before departing on the transport mission.

(1) A courier certification memorandum is a unit-originated memorandum that officially designates specific personnel to act as CCI couriers. DD Form 2501 is not required to transport an unkeyed CCI.

(a) The certification memorandum is valid anywhere as long as the means of transportation is U.S. Government-owned or -contracted.

(b) If emergency situations dictate that a privately owned vehicle (POV) must be used, the commander will include the statement, "Government transportation is not available or waiting for it would cause grave damage to the mission" on the certification memorandum.

(c) The courier will carry the certification memorandum on his or her person throughout the mission.

(2) If mission time constraints require the courier to use a non-U.S. flag carrier or U.S. commercial airline to perform the mission, a request for exception to policy signed by the first colonel (O6) in the chain of command must be submitted to the USAREUR G2 (AEAGB-SAD-S), Unit 29351, APO AE 09014-9351. The PLA is CDRUSAREUR HEIDELBERG GE//AEAGB-SAD-S// (this reg, fig 1).

(3) A courier certification memorandum is not required for CCIs installed in crew vehicles or aircraft engaged in training or operations.

NOTE: Transportation of CCIs for turn-in at the General Support Center, Europe (GSC-E), security warehouse in Kaiserslautern, will follow guidance in paragraphs C-6a and C-7.

b. Registered Mail. Only United States Postal Service (USPS) registered mail will be used for lateral transfer or return of CCIs still under warranty to a manufacturer. No other mailing service, to include FedEx and UPS, will be used in the European region to mail CCIs. CCIs cannot pass through a foreign postal system or receive a foreign inspection.

(1) Addressing CCI registered mail packages to Army post office (APO) or Fleet post office (FPO) destinations meets this requirement.

DEPARTMENT OF THE ARMY
COURIER'S UNIT
UNIT 12345
APO AE 09000-2345

AEAXX-XX (Date)

MEMORANDUM FOR RECORD

SUBJECT: CCI Courier Certification

1. I certify that I have a valid U.S. Secret security clearance and have been briefed and understand my responsibilities as a controlled cryptographic item (CCI) courier. These responsibilities include--

a. Checking numbers and quantities of CCIs against the material receipt.

b. Ensuring continuous protection of CCIs.

c. Keeping in my possession CCI courier orders, exception-to-policy memorandums (if applicable), and all other required authorization and documentation.

d. Ensuring that the CCI material is properly packed and sealed for transport. (When packed in a durable, sealed, opaque container, the equipment may be transported aboard a commercial airline as checked baggage.)

e. When transporting CCI material by U.S. Government ground transportation, I will brief the driver on the mission and responsibilities of safeguarding highly sensitive material. I will choose U.S. Government installations when available for stops and inspect the CCI material container after each stop.

f. I will allow customs officials and airport security personnel to inspect the container, including the CCI material. This is done to meet customs and international airline safety requirements. However, inspections must be done in my presence, and the equipment must remain in my physical control. If the container is opened for inspection, it must be resealed or secured before further transport.

g. Under no circumstances will I attempt to conceal the CCI material from officials or make any statement or gestures that may be threatening or demanding. I will not attempt to use force to protect the material, make false or misleading statements, or in any way evade required inspections.

2. During an emergency, I will be responsible for--

a. Ensuring continuous control and protection of the material.

b. Destroying the material when compromise is eminent (under hostile conditions).

c. Notifying the nearest U.S. military installation or facility and my unit.

3. I understand and acknowledge my responsibilities as a courier for CCIs as indicated.

COMMANDER/REPRESENTATIVE	COURIER
(Signature)	(Signature)
Name:	Name:
Rank:	Rank:
Title:	Title:

Figure C-1. Sample CCI Courier Certification Memorandum

(2) Packaged CCIs may not exceed size and weight limits for registered mail.

(3) CCIs will be single-wrapped and will have two-inch lettering "CCI" in plain view.

NOTE: Routine theater distribution center movements do not meet CCI criteria (seals and signature control) and will not be used to transport CCIs in the European region.

C-7. CCI TURN-IN PROCEDURES

a. CCIs will be turned-in only to the GSC-E security warehouse (RIC WQD DODAAC W80Q7B). If a CCI is inadvertently picked up by an SSA stock record account, the SSA account holder will generate an automated request for disposition.

(1) European region class 7 item managers and unit SSAs in the European theater (including those managers at Task Force Eagle and Task Force Falcon) will turn in CCIs to the GSE-E security warehouse as prescribed in this appendix.

(2) CCIs will not be placed in unmarked multipack containers with non-CCI material and shipped to the GSE-E Central Receiving Facility, a Defense Reutilization and Marketing Office, or the Pirmasens Communication and Electronics Facility. Mixed shipping is a CCI incident and must be reported through channels as prescribed in the basic regulation, paragraph 12d. CCI will be transported by courier to the Kaiserslautern GSE-E security warehouse with proper turn-in documentation as prescribed in paragraph C-8b.

b. Unit PBOs are responsible for screening and identifying CCI before it is turned in.

(1) Unit PBOs will ensure equipment and serial numbers are reported according to AR 710-3, section V. PBOs will ensure that their units follow the guidelines in (2) through (4) below when turning in CCIs.

(2) Unit PBOs are not authorized to ship CCIs directly to Tobyhanna Army Depot (TYAD). CCI coded "Not Repairable This Station" during a technical inspection (TI) will be hand-carried for turn-in to the GSC-E security warehouse.

(3) Unit PBOs will contact the supporting material management center (MMC) for disposition instructions on excess or nonrepairable CCIs.

(4) Units will not turn in CCIs to the GSC-E security warehouse without disposition instructions.

(a) The GSC-E security warehouse will accept the CCI for turn-in only when the CCI is 100-percent complete or accountability is documented for all components. A shortage annex signed by the unit commander is required for missing components. A report of survey is required for missing major end items.

(b) DA Pamphlet 25-380-2 provides guidance on shipping or transporting CCIs. This appendix provides specific guidance for the European region. AR 710-3 governs UIT of CCI. For CCI items, CIIC 9 and accounting requirement code N (nonexpendable) are reportable to UIT. CCI FILL devices are not reportable to the UIT Program according to AR 710-3. All CCI end items (including nonreportable CCI FILL devices), however, must be accounted for by serial number on unit property book records. The PBO or unit supply sergeant normally will perform the UIT function.

C-8. PREPARING CCI FOR TURN-IN

Only trained unit personnel will prepare CCI for turn-in.

a. Zeroization. Once CCI is zeroized, the batteries will be removed from the item before turn-in (except for STU-IIIs). The battery covers will be left open or off. The batteries cannot be removed from some STU-IIIs (for example, the AT&T 1100 and 1150). Most CCIs will automatically zeroize if the batteries are removed for more than 1 minute. However, removing the batteries from a CCI does not ensure the equipment is zeroized. CCIs must be manually zeroized before turn-in. With the exception of the KYK-13, KYX-15A, and CYZ-10, electric power must be supplied to the CCI for the zeroization process. To zeroize--

(1) The KYX 15A and KY57: Place the selector switch in the "Z ALL" position and press the initiate button.

(2) The KY-99/KY-99A: Select the "Z ALL" switch, pull it out, and turn it.

(3) The KG-84: Pull the “ZEROIZE” switch out and down.

(4) The KG-194: Select “ZEROIZE” or “ACTUATE.”

(5) The AN/CYZ-10 Data Transfer Device (DTD): Push the “ZEROIZE” button three times.

(6) The KYK-13: Place the selector switch in the “Z ALL” position.

(7) The RCA model STUG: Push the “ZEROIZE” switch (located in back of the STU-III) to the right, then back to the left.

(8) The GTE 9600: Press “MENU” or “DELETE.” After a short pause, the screen will display: “View KSD.” Press “Yes” to complete the zeroization.

(9) The Motorola SECTEL 1500: Lift the flap above the handset and press the red button.

(10) The AT&T STU-III: Push a paperclip into the hole next to the word “ZEROIZE.”

b. Documentation.

(1) The assigned PBO (or primary hand-receipt holder) and unit commander of the activity turning in CCI equipment will prepare the following documents:

(a) DD Form 1348-1A. The DD Form 1348-1A must be typed and error-free with no more than 10 serial-number items per document and signed by the PBO or commander. DA Form 2765-1 may be used in place of DD Form 1348-1A.

(b) DA Form 2407.

(c) Verification of zeroization memorandum. (Figure C-2 shows a sample.) This document will state that correct turn-in procedures have been followed and verify that the CCI has been zeroized. The memorandum will include the unit address, the Department of Defense activity address code (DODAAC), the nomenclature, serial number, and document number for each CCI turned in. The commander or PBO will sign the memorandum, which will be hand-carried throughout the turn-in process.

(d) DA Form 1687 for the unit commander. Individuals turning in the CCI to GSC-E security warehouse (unit-designated courier) must be on the current signature card.

(e) Assumption-of-command orders. If applicable, these orders will also accompany turn-in documents.

(f) DD Form 1348-2.

(g) DD Form 1577-2 or DD Form 1574, if applicable.

(2) Because CCI is sensitive, turn-in documentation must be error-free. Documentation with mistakes will be rejected.

(3) The turn-in documents listed in (1) above will be hand-carried with the CCI to the GSC-E security warehouse. The GSC-E security warehouse will accept faxed copies of the turn-in documents in (1) above, except DD Form 1348-1. This exception keeps units from having to make more than one trip to the GSC-E security warehouse if turn-in documents are incomplete.

C-9. INSPECTION AND TURN-IN PROCEDURES (UNIT TO GSC-E SECURITY WAREHOUSE)

a. PBOs or hand-receipt holders turning in CCIs will take the DA Form 2407 (para C-8b) and the CCI that is to be turned in to their direct support unit (DSU) or CMDSA for a TI. The TI will include a serviceability check and verification of zeroization before turning in the CCI at the GSC-E security warehouse.

DEPARTMENT OF THE ARMY
UNIT TURNING IN CCI
UNIT 12345
APO AE 09000-2345

AEAXX-XX (Date)

MEMORANDUM FOR Security Items Branch, GSC-E Security Warehouse (SAK), CMR 429, APO AE 09054-0429

SUBJECT: Verification of Zeroization of Controlled Cryptographic Items (CCI)

1. I certify that the CCIs listed below `have been zeroized by a qualified COMSEC technician and are being turned in unkeyed according to AR 380-40, paragraph 2-16b.

STU-III (STUG30)	C2345XX	W81KDP61640333
KYX-15A/TSEC	C5678XX	W81KDP61640334
ELECT KEY KYK-13/TSEC	C7890XX	W81KDP61640335
Radio Set RT-1527A	12798XX	W81KPD61640336

2. I fully understand that failure to ensure that the listed CCIs are properly zeroized will result in a reportable COMSEC incident.

3. Equipment is zeroized and has been inspected by our supporting DSU or CMDSA. The CCI listed above has not been rekeyed or used since the technical inspection.

JOHN A. SMITH
Captain, IN
Commanding

GSC-E Security Warehouse Date Accepted

Accepted by: (Print) Last Name First Name MI Signature

Figure C-2. Sample Verification of Zeroization Memorandum

b. A DSU or CMDSA representative will authenticate the DA Form 2407 by printing or typing “Zeroized in accordance with AE Regulation 380-40” on the form and by typing or printing his or her name, rank, title, and telephone number on the form and signing it. The DSU or CMDSA representative will also make the same annotation in the Remarks block of the serviceability tag (DD Form 1577, DD Form 1577-2, or DD Form 1574) if a tag is used.

NOTE: Use of CCI equipment after completion of TI by DSU or CMDSA invalidates the DA Form 2407 authenticated for validation of zeroization.

c. The unit courier will then hand-carry the CCI to the GSC-E security warehouse. The GSC-E security warehouse is located at the Supply Activity Kaiserslautern (SAK), building 2370, Kaiserslautern, Germany. For turn-in appointments, call DSN 483-8820 or civilian 0631-411-8820, Monday, Tuesday, Wednesday, and Friday, 0730 through 1145. Appointments are not available on Thursday. The nonsecure fax for the security warehouse is DSN 483-7772.

d. GSC-E security warehouse personnel will not accept CCIs without required (correctly and completely filled out) documentation. All CCI must be free of dirt before turn-in.

e. GSC-E security warehouse personnel will check signature records of persons who have had accountability and custody from the pick-up point to the drop-off point (para C-8b).

C-10. GSC-E TURN-IN PROCEDURES TO TYAD

a. GSC-E security warehouse personnel will accept CCIs for turn-in. They will stamp and sign the payroll signature on documentation in the appropriate blocks on turn-in forms.

(1) One copy of the stamped turn-in document (DD Form 1348-1A or DA Form 2765-1) and a copy of the verification of zeroization memorandum (fig C-2) will be stored with the associated CCI.

(2) The remaining copies will be sent to the accountable officer requesting disposition instructions. When final disposition on the CCI is received and the CCI is prepared to be shipped out of the GSC-E security warehouse, the documentation will be checked a second time to ensure accuracy and completeness.

b. Once a DD Form 1348-1A or DA Form 2765-1 is generated for a CCI, the GSC-E security warehouse personnel will verify the item and its documents. GSC-E security warehouse personnel will compare the CCI to turn-in documentation and the verification-of-zeroization memorandum. GSC-E security warehouse personnel will ensure documents provide required information and are signed by the PBO or primary hand-receipt holder.

c. When the procedures in subparagraph b above are completed, GSC-E security warehouse personnel will annotate the verification-of-zeroization memorandum with the date of the transaction.

d. When the GSC-E security warehouse ships CCI to TYAD, a copy of the verification-of-zeroization memorandum, a copy of the DD Form 1348-1A or DA Form 2765-1, and a copy of the DA Form 2407 will be kept and filed by the GSC-E security warehouse personnel (AR 25-400-2).

e. Each unit's CCI accepted for shipment to TYAD will be stored together in one area (preferably the same bin) at the GSC-E security warehouse.

f. DA Pamphlet 25-380-2 prescribes wrapping and marking requirements and shipping instructions for CCI. GSC-E security warehouse personnel will ship CCI according to DA Pamphlet 25-380-2 and this regulation.

g. Each unit's CCI accepted for shipment will be shipped to TYAD in the same crate when possible.

h. GSC-E security warehouse personnel will attach a copy of the verification-of-zeroization memorandum, a copy of the DA Form 2407, and a copy of the DD Form 1348-1A or DA Form 2765-1 (showing the DODAAC of the unit that turned in the CCI) to the container with that unit's CCI equipment.

i. GSC-E security warehouse personnel will return CCI to TYAD for final disposition, regardless of its condition.

GLOSSARY

SECTION I
ABBREVIATIONS

AE	Army in Europe
ALC	accounting legend code
APO	Army post office
AR	Army regulation
AUTODIN	automatic digital network
CCI	controlled cryptographic item
CCIR	Change of Custodian Inventory Report
CF	central facility
CG, USAREUR/7A	Commanding General, United States Army, Europe, and Seventh Army
CIIC	controlled item inventory code
CIK	cryptoignition key
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CMCS	COMSEC Material Control System
CMDSA	COMSEC material direct support activity
COMSEC	communications security
CONAUTH	controlling authority
CONUS	continental United States
CPA	card privilege authority
DA	Department of the Army
DACAP	Department of the Army Cryptographic Access Program
DCS	Defense Courier Service
DD	Department of Defense (form)
DEROS	date eligible for return from overseas
DMS	Defense Message System
DOD	Department of Defense
DODAAC	Department of Defense activity address code
DS	direct support
DSN	Defense Switched Network
DSU	direct support unit
DTD	data transfer device
DTG	date time group
EKMS	Electronic Key Management System
FPO	Fleet post office
G2	Deputy Chief of Staff, G2, USAREUR
G3	Deputy Chief of Staff, G3, USAREUR
G4	Deputy Chief of Staff, G4, USAREUR
G6	Deputy Chief of Staff, G6, USAREUR
GPS	Global Positioning System
GS	general support
GSA	General Services Administration
GSC-E	General Support Center, Europe
GSM-SM	Global System for Mobile Communications-Security Module
HQ USAREUR/7A	Headquarters, United States Army, Europe, and Seventh Army
HQDA	Headquarters, Department of the Army
IAM	information assurance manager
IASO	information assurance security officer
INSCOM	United States Army Intelligence and Security Command
KG	key generator
KMC	key management center
KSD	key storage device
LCMS	local COMSEC management software
LN	local national
MMC	material management center
NATO	North Atlantic Treaty Organization

NDA	national distribution authority
NSA	National Security Agency
OTAD	over-the-air-key distribution
OTAR	over-the-air-rekey
PBO	property book officer
PIN	personal identification number
PLA	plain language address
POC	point of contact
POV	privately owned vehicle
QPI	Quarterly Possession Inventory
RCERT-E	Regional Computer Emergency Response Team, Europe
RCS	requirement control symbol
S2	intelligence officer
SAIR	Semiannual Inventory Report
SAK	Supply Activity Kaiserslautern
SBU	sensitive but unclassified
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SDNS	Secure Data Network System
SF	standard form
SIR	serious incident report
SOP	standing operating procedure
SSA	supply support activity
STE	secure terminal equipment
STU-III	secure telephone unit, third generation
TB	technical bulletin
TCMO-E	Theater Communications Security Management Office, Europe
TEK	traffic encryption key
TI	technical inspection
TPA	terminal privilege authority
TPI	two-person integrity
TS	Top Secret
TYAD	Tobyhanna Army Depot
U.S.	United States
UIT	unique item tracking
UR	USAREUR regulation
US/FORN	United States/foreign nationals
US/UK	United States/United Kingdom
USACCSLA	United States Army Communications-Electronics Command Communications Security Logistic Activity
USAREUR	United States Army, Europe
USEUCOM	United States European Command
USPS	United States Postal Service
VTAADS	Vertical--The Army Authorization Documents System

SECTION II
TERMS

access
Uncontrolled physical possession that provides an opportunity to gain detailed knowledge about the controlled cryptographic item.

authorized personnel
All of the following:

● U.S. citizens who are U.S. Government employees.

● U.S. citizens who are U.S. Government contractors.

● U.S. resident aliens who are U.S. Government civilian employees or are members of the U.S. active or reserve armed forces.

● Local nationals (military or civilian) employed by U.S. Government agencies or their respective governments (only with a U.S. Government escort).

controlled cryptographic items
Unclassified (but controlled) high-value, sensitive controlled communications security (COMSEC) equipment that requires protection against unauthorized access, because it contains an embedded logic that performs cryptographic functions. Controlled cryptographic items (CCIs) are identified by the controlled item inventory code 9 (CIIC 9) in the FEDLOG. As sensitive items, specific safeguards and procedures must be followed to ensure that physical security requirements are met. DA Pamphlet 25-380-2 provides detailed guidance on shipping and transporting CCI. AR 710-2 contains logistic control guidance. AR 710-3 governs unique item tracking for CCI.

embedded CCI
A cryptographic component designed and engineered to be incorporated into unclassified communication or information processing equipment or system to form a controlled cryptographic item (CCI) end item.

● The host equipment may process voice, data, or record communications. The CCI component provides the equipment with a cryptographic capability.

● Normally the CCI component is embedded within the host equipment and is not readily identifiable by the user. For this reason, the serial number of the host equipment must be used for accounting purposes.

● The CCI component cannot perform any function by itself. The component obtains its power from the host equipment.

● An embedded CCI component may take a variety of forms, such as a module, a printed circuit card or board, microcircuit, or a combination of these items.

● Only qualified technicians are authorized to install or remove a CCI component from the host equipment.

installed CCI
Equipment set up and available for use (for example, an unkeyed KY-57 installed as part of a radio system in a high mobility multipurpose wheeled vehicle).

no-lone zone
An area, room, or space that, when staffed, must be occupied by two or more appropriately cleared individuals who remain within sight of each of other.

uninstalled CCI
Controlled cryptographic equipment held in storage as a separate item (for example, a spare unkeyed KY-57, an unkeyed KYK-13, an unkeyed AN/CYZ-10 stored in a sensitive-items cage in a locked supply room).