Headquarters
United States Army Europe
Wiesbaden, Germany

Headquarters
United States Army Installation Management Command
Directorate-Europe
Sembach, Germany

Army in Europe
Regulation 380-40*

1 February 2017

Security

Safeguarding and Controlling Communications Security Material

***This regulation supersedes AE Regulation 380-40, 25 November 2013**

For the Commander:

KAI R. ROHRSCHNEIDER
Brigadier General, GS
Chief of Staff

Official:

DWAYNE J. VIERGUTZ
Chief, Army in Europe
Document Management

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

Summary of Change. The revision—

- Revises controlled cryptographic item turn-in procedures (para 7).

- Adds Procedures for loading COMSEC into NATO and Coalition Partner Nations End Cryptographic Unit Devices (para 16).

Applicability. This regulation applies to Army organizations supported by USAREUR that handle COMSEC material in the USEUCOM and USAFRICOM theaters.

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. Record titles and descriptions are on the Army Records Information Management System website at *https://www.arims.army.mil*.

Supplementation. Organizations will not supplement this regulation without approval of the Security Branch, Intelligence Support Division, Office of the Deputy Chief of Staff, G2, HQ USAREUR.

Forms. This regulation prescribes AE Forms 380-40D and 380-40F. AE and higher-level forms are available through the Army in Europe Library & Publishing System (AEPUBS) at *http://www.eur.army.mil/aepubs/*.

Suggested Improvements. The proponent of this regulation is the Security Branch, Intelligence Support Division, Office of the Deputy Chief of Staff, G2, HQ USAREUR (mil 537-2104). Users may send suggested improvements to this regulation by e-mail: *usarmy.badenwur.usareur.list.g2-isd-sso-security@mail.mil*.

Distribution. This regulation is available only electronically and is posted in AEPUBS at *http://www.eur.army.mil/aepubs/*.

CONTENTS

1. PURPOSE

This regulation prescribes policy and assigns responsibilities for safeguarding and controlling communications security (COMSEC) material in the USEUCOM and USAFRICOM areas of operation. This regulation also provides guidance on programming and installing secure terminal equipment (STE) and the Timeport 280 Global System for Mobile Communication - Security Module (GSM-SM) (secure cell phone) in private quarters. This regulation must be used with AR 25-2, AR 380-40, and TB 380-41.

2. REFERENCES

Appendix A lists references.

3. EXPLANATION OF ABBREVIATIONS

The glossary defines abbreviations.

4. RESPONSIBILITIES

a. The USAREUR G2 will—

(1) Establish policy and procedures for safeguarding and controlling COMSEC material in the USEUCOM and USAFRICOM theaters and conducting command COMSEC-facility inspections.

(2) Be the proponent for the COMSEC Account Managers Course (INT 34) and the Local COMSEC Management Software (LCMS) Course (INT 35). The USAREUR G2 will also be the final authority in the USEUCOM and USAFRICOM theaters for the following:

(a) Validating annual training needs (AE Reg 350-1).

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

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

(3) Manage the Cryptographic Access Program (CAP).

(4) Manage the Army in Europe COMSEC Incident Program.

(5) Prepare and issue reports on COMSEC-incident trends.

(6) Appoint a command COMSEC inspector.

(7) Conduct command COMSEC inspections of commands throughout the Army in Europe.

(8) Review and approve or deny the transportation of COMSEC material by non-U.S.-flag carriers.

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

(10) Review and approve or deny requests for exceptions to Army policy on controlled cryptographic items (CCIs).

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

(12) Help develop Army in Europe COMSEC policy.

(13) Develop and publish procedures for command inspections of COMSEC facilities in Europe.

(14) Review COMSEC-incident reports to—

(a) Determine the effects of COMSEC incidents on operations and provide guidance on recovery actions.

(b) Revise or develop procedures to improve security and prevent incidents.

(15) Coordinate with the Office of the Deputy Chief of Staff, G6, HQ USAREUR, before issuing guidance from DOD, HQDA, and national organizations responsible for COMSEC.

(16) Distribute, in coordination with HQDA, instructions on the disposal of CCIs.

b. The USAREUR G3/5/7 will establish priorities for distributing COMSEC equipment and CCIs.

c. The USAREUR G4 will—

(1) Perform the requirements of the Unique Item Tracking Program (AR 710-3) on behalf of USAREUR.

(2) Act as the lead for resolving COMSEC incidents involving CCIs at depots and other logistic facilities throughout the Army in Europe.

(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) Serve as the staff proponent for property accountability of CCIs.

d. The USAREUR G6 will—

(1) Conduct, in coordination with the USAREUR G2, command COMSEC inspections for USAREUR COMSEC accounts.

(2) Perform COMSEC command authority responsibilities for USAREUR.

(3) Help the USAREUR G2 develop Army in Europe COMSEC policy.

(4) Represent USAREUR in the Army Cryptographic Modernization Initiative.

(5) Provide COMSEC guidance for exercises and contingency plans.

(6) Approve increases or decreases in keying material for USAREUR and subordinate unit COMSEC accounts when required.

(7) Approve the establishment and deactivation of COMSEC accounts for USAREUR and its subordinate units.

(8) Help USAREUR and its subordinate units resolve COMSEC account-management issues.

(9) Be the proponent for fielding tactical cryptographic systems and ensure that users order and receive cryptographic keys for those systems.

e. The Commander, 181st Signal Company, will—

(1) Manage the United States Army Theater COMSEC Management Office, Europe, as the theater COMSEC logistic support facility for storage and distribution of cryptographic keys and classified COMSEC Material Control System hardware.

(2) Provide theater COMSEC logistic (supply) support to organizations in the European theater, other military departments, U.S. Government agencies, NATO, and other allies. This requires providing a centralized storage and distribution point for positive-controlled material to support USEUCOM and other Army organizations in the European theater.

(3) Send operational-necessity requests for approval to transport COMSEC material by courier aboard a civilian carrier to CDRUSAREUR DCSINT WIESBADEN GE//AEIN-IS// (for electronic messages) or *usarmy.wiesbaden.usareur.list.g2-isd-sso-security@mail.mil* (for e-mail).

f. Commanders supported by a U.S. Army COMSEC account will execute the responsibilities in AR 380-40, paragraph 1-13, and do the following:

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

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

g. The Commander, 21st Sustainment Command (21st SC), will track CCI property (AR 710-3, chap 4) in the European theater.

5. RESOLVING CONFLICTS

a. Commanders should refer to Department of the Army (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 (AEIN-IS), Unit 29351, APO AE 09014-9351.

6. TRANSPORTING COMSEC AND CCI MATERIAL ABOARD NON-U.S.-FLAG AIRCRAFT

a. Exception-to-policy requests to use non-U.S.-flagged commercial aircraft to transport COMSEC key and equipment (fig 1) must be sent to the USAREUR G2 (AEIN-IS), Unit 29351, APO AE 09014-9351, or by e-mail to *usarmy.wiesbaden.usareur.list.g2-security-office@mail.smil.mil*. Requests must include the following:

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

(2) A statement that all other options to meet keying requirements (for example, over-the-air-rekey, local COMSEC accounts) were examined and determined to be unsuitable.

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

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

b. Commanders will use DD Form 2501 to appoint unit personnel as official unit couriers to transport classified COMSEC material outside United States Army garrisons and field operating sites within the same country in accordance with AR 380-5, chapter 8, and USAREUR Supplement 1. (DD Form 2501 is an accountable form valid for 1 year after the date of issue.)

7. CCI TURN-IN PROCEDURES

a. The losing unit will turn in CCI through the local supply support activity (SSA). The Theater Logistics Support Center-Europe (TLSC-E) Security Warehouse will not accept turned-in CCIs unless equipment is processed through the Supply Support Activity's Global Combat Support System-Army (GCSS-A) before being turned in.

b. The SSA will process equipment in the GCSS-A and direct equipment to the TLSC-E Security Warehouse; Ludwigshafener Straße 31, 67657 Kaiserslautern, Germany; DOD activity address code (DODAAC): W80Q7B; Routing Identifier Code (RIC): WQD; military 483-8117/8183, civilian 0631-483-8117/8183. AR 380-40 prescribes security procedures for handling CCIs.

c. Users and unit supply personnel must ensure that equipment is zeroized and batteries are removed from legacy equipment before turning in CCIs. The TLSC-E Security Warehouse will ship the equipment to the Tobyhanna Army Depot (TYAD) with a statement confirming that a technical inspection was not conducted. Users and PBOs will ensure that CCIs include a memorandum verifying zeroization (fig 2) before turning the items in to the SSA. SSAs will forward the zeroization memorandum, the Federal logistics data, the turn-in document, the certification-of-hard-drive disposition, DLA Form 2500 if required, and other pertinent documents in subparagraphs d through g below to the TLSC-E Security Warehouse.

d. Before a unit turns in CCIs, the unit must manually zeroize the CCI and remove the batteries after zeroization. Battery covers must be left open or removed. Most CCIs will automatically zeroize when the batteries are removed for more than 1 minute. Removing the batteries does not, however, ensure that the equipment is zeroized. The losing unit must complete DLA Form 2500 if hard drives were removed.

e. The verification-of-zeroization memorandum must state that correct turn-in procedures have been followed and verify that the CCIs have been zeroized. The memorandum must include the losing unit's address and the DODAAC as well as the nomenclature, serial number (SN), and document number for each CCI that is turned in. The unit commander or PBO will sign the memorandum, which must be hand-carried throughout the turn-in process.

f. CCIs will not be placed in unmarked, multipack containers with non-CCI material and shipped to the TLSC-E Central Receiving Facility. CCIs will be transported by courier to the Kaiserslautern TLSC-E security warehouse with proper turn-in documentation.

g. Unit PBOs are responsible for screening and identifying CCIs before they are turned in. Unit PBOs or commanders will—

(1) Ensure equipment and SNs are reported in accordance with AR 710-3, chapter 2, section IV, paragraph 2-50, table 2-6 and table 2-7.

(2) Ensure CCIs are hand-carried to the local SSA, and ensure that couriers have courier cards when turning in Secret CCI. The TLSC-E Security Warehouse will ship CCIs to TYAD. Items must be cleaned and transported in Government vehicles.

(3) For instructions on disposing of excess or nonrepairable CCIs, units may contact the 21st SC, Class 7 Section, at military 484-7820/8021.

(4) Ensure CCIs are not turned in to the SSA without disposition instructions.

(5) Provide DA Form 1687 authorizing individuals to turn in CCIs. Commanders and PBOs may contact their local SSA for additional turn-in requirements.

(6) Provide a copy of the commander's assumption-of-command orders or the PBO orders to the SSA to be forwarded to the TLSC-E Security Warehouse.

(7) Ensure DD Form 1348-1A is prepared in a printed and error-free manner with no more than 10 SNs per document and sign the form in the bottom left corner. In the absence of an official stamp, "PBO" must be written by the signatory's name to confirm that the signatory is the PBO.

NOTE: A delegation-of-authority memorandum from the PBO authorizing others to sign DA Form 1348-1A will not be accepted.

(8) Ensure financial liability investigations of property loss reports are provided for damaged items and major end items.

(9) Ensure that their units follow the guidelines on turning in CCIs. The TLSC-E security warehouse will accept CCIs for turn in only when the CCIs are 100-percent complete or accountability is documented for all components. A shortage annex signed by the unit commander or PBO is required for missing components. Property adjustments are required for major items following the procedures in AR 735-5. Unit commanders or PBOs may schedule a turn-in by calling military 483-8117/6690.

[SECURITY CLASSIFICATION]

DEPARTMENT OF THE ARMY
UNIT
UNIT #####
APO AE *xxxxx-xxxx*

(Office Symbol) *(Date)*

MEMORANDUM FOR USAREUR G2 (AEIN-IS), Unit 29351, APO AE 09014-9351

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

1. (U) References:

a. (U) AR 380-40, Safeguarding and Controlling Communications Security Material.

b. (U) AE Regulation 380-40, Safeguarding and Controlling Communications Security Material.

2. (U) In accordance with the references in paragraph 1, authority is requested to hand-carry COMSEC material aboard a non-U.S.-flag aircraft from Frankfurt, Germany, to Bucharest, Romania, on or around 10 November 2017. The return flight will be on the same airline on or around 27 November 2017. The mission is in support of a survey and investigation pertaining to the recovery of World War II Soldiers buried in Romania.

3. (U) 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. (U) Type of Material: three automated net control devices, one precision lightweight Global Positioning System (GPS) receiver, AKAD A1105, and ALC-1 key. The controlling authority is the United States Army 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. Soldiers. All other options to meet keying requirements were examined and determined unsuitable. The COMSEC manager will load the key onto the GPS receiver before the time of travel.

5. (U) The 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) The POC is Mr. Smart, military 484-2222.

BERNARD F. HILL
Colonel, IN
Commanding

[SECURITY CLASSIFICATION]

Figure 1. Sample Exception-to-Policy Request to Transport COMSEC and CCI Material Aboard Non-U.S.-Flag Aircraft

DEPARTMENT OF THE ARMY
(*UNIT NAME*)
(*UNIT NUMBER*)
APO AE *XXXXX-XXXX*

(*Office symbol*) (*Date*)

MEMORANDUM FOR Security Items Branch, TLSC-E Security Warehouse, CMR 429,
APO AE 09054-0429

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

1. References:

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

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

2. I certify that the following CCIs have been zeroized and are being turned in unkeyed in accordance with AR 380-40, paragraph 8-18b:

KG 175	SN:	DODAAC: W81KDP	3032-0001
KG 75	SN:	DODAAC: W81KDP	3032-0002

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

4. The POC is (*name*), military *XXX-XXXX*, civilian *XX-XXXX-XX-XXXX*, e-mail (Unclas): (*first name*).(*last name*).(*[civ][mil]*)@mail.mil.

NAME
Rank, Br
Commanding [or PBO]

TLSC-E Security Warehouse:

Date accepted: _____ Accepted by: _____[Signature]_____
Last name, first name [print]

Figure 2. Format for a Verification of Zeroization Memorandum

8. CONTINUITY-OF-OPERATION PLAN

All units with COMSEC accounts must have a continuity-of-operation plan (COOP). This plan will be used to back-up and transfer operations.

a. The COOP must—

(1) Include detailed instructions for account personnel, be exercised (tested) annually, and revised if required. The annual exercise (test) will be documented.

(2) Be tailored to the organization, its mission, and operational environment, and address concerns identified in risk assessments conducted by the responsible commander in accordance with AR 190-51.

b. The COOP will not be an item of interest during Communications Security Logistics Activity (CSLA) audits. However, the COOP will be inspected and evaluated during all command COMSEC inspections.

c. DA Pamphlet 25-1-1 provides guidance on developing COOPs.

9. COMMAND COMSEC INSPECTIONS

a. 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 of each inspection to the USAREUR G2 (AEIN-IS), Unit 29351, APO AE 09014-9351.

b. The command COMSEC inspector will send inspection reports to the inspected unit within 20 workdays after the inspection. Units with deficiencies will have 30 calendar days to reply. The reply must describe the corrective actions taken. When deficiencies cannot be resolved within 30 days, an interim reply is required.

c. The inspected unit will send a copy of the basic report and the reply to the inspecting unit or investigator by the suspense date. The inspected unit will also send a copy of the report and the reply to the commander of the next higher headquarters for review.

d. The next higher headquarters above the inspected unit will ensure that the corrective actions will be completed or in progress before it endorses the reply through command channels to the inspecting office.

10. COMSEC-INCIDENT REPORTING

a. To help users of COMSEC material submit incident reports, the CSLA released a web-based system on the SIPRNET at *https://cslamissionapps.army.smil.mil*. The site requires an Army Knowledge Online SIPRNET login. To report a COMSEC incident, users must click on the *COMSEC Incident Monitoring Management System* link.

b. Message addressees for European-theater COMSEC incident reports (AR 380-40, chap 7) are as follows:

(1) Physical, Cryptographic, and Personnel Incidents:

ACTION ADDRESSEES:
CONAUTH
CSLA INCIDENTDESK(sc)
INFO:
HIGHER HQ AS DIRECTED BY UNIT STANDING OPERATING PROCEDURE (SOP)
DIRNSA FT GEORGE G MEADE MD//I413//
USAREUR G6(sc)
USAREUR G2(sc)
66MI OCE CI (sc)

(2) Administrative Incidents Addressed in AR 380-40, Chapter 6:

ACTION ADDRESSEE:
CONAUTH
INFO:
HIGHER HQ AS DIRECTED BY UNIT SOP
USAREUR G6(sc)
USAREUR G2(sc)

c. CCI incidents in the European theater will be reported as follows:

(1) CCI users will report CCI incidents to their unit PBO.

(2) On receiving a report of a CCI incident, the PBO will—

(a) Prepare a CCI-incident report as prescribed by TB 380-41.

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

ACTION ADDRESSEES:
CDR LOGSA (sc)
INFO:
DIRNSA FT GEORGE G MEADE MD//I01P3//
HIGHER HQ AS DIRECTED BY UNIT SOP
USAREUR G6(sc)
USAREUR G2(sc)
66MI OCE CI (sc)

d. According to CJCSI 3260.01C, COMSEC incidents involving positive-controlled (keyed) material will be reported to EUCOM J36 Command and Control Div(mc) as an action addressee.

11. SECURE TERMINAL EQUIPMENT AND TIMEPORT 280 GSM-SM (SECURE CELL PHONE) INSTALLATION AND USE IN PRIVATE QUARTERS

a. Secure Terminal Equipment (STE).

(1) Only high-level officials (general officers, brigade commanders, certain battalion commanders, and DOD civilian equivalents) are authorized STE in their private residences.

(a) Classified discussions are not authorized in most private quarters. In nonsecure areas (for example, residences), the residential user is restricted to listening to classified information (listen mode only). Unless appropriate storage is available, any notes taken by the residential user during these conversations must be limited to unclassified information. In addition, because the residential environment is not secure, all comments made must be limited to the unclassified level.

(b) A nonresidential user must verify the identity of the residential user and observe clearance-level and need-to-know restrictions before discussing any classified information. No classified calls will be initiated from a private residence unless previously cleared for classified discussions in accordance with AR 381-14 and AE Regulation 380-85.

NOTE: When ordering key for residential installation, the supporting COMSEC account must be notified of its intended use so that *RESIDENCE* can be included in the information to be displayed.

(2) Unit security managers will certify the installation of an STE in an authorized residence by sending a memorandum to USAREUR G2 (AEIN-IS), Unit 29351, APO AE 09014-9351, certifying installation of the STE. The memorandum will include the resident's name, position, and residential address (fig 3). This memorandum will be used to ensure accountability for the COMSEC key (KSV-21) in private quarters throughout the European theater and help the Army in Europe COMSEC Incident Program Manager keep an up-to-date database of KSV-21 cards and the Timeport 280 GSM-SM in private quarters.

(3) The unit security manager is responsible for ensuring KSV-21 cards and GSM-SMs are returned to the COMSEC account and for notifying the Security Branch, Office of the Deputy Chief of Staff, G2, HQ USAREUR, when officials who have COMSEC key for residential STE depart the organization permanently or when the STE is no longer needed.

(4) STE may be installed in the private quarters of designated high-level officials during their service in their specific positions.

(5) If STE in private quarters is approved (certified), the following standards and conditions must be met:

(a) Audio and physical-security precautions must prevent unauthorized access to the STE and the key (KSV-21 or GSM) and must prevent information from being intercepted. STE in private quarters will not be used as a standard telephone, and precautions for use of the STE must meet DOD security standards for protecting information.

(b) Requests to certify certain private quarters for classified two-way discussions (AR 381-14) will be made in accordance with AE Regulation 380-85, appendix B. The certification becomes void if an uncleared person enters the quarters with unescorted access. Figure 4 provides the Secure Telephone Certification/Recertification, Residence Inspection Checklist.

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

AEAQ-IS-S 18 August 2016

MEMORANDUM FOR USAREUR G2 (AEIN-IS), Unit 29351, APO AE 09014-9351

SUBJECT: Secure Terminal Equipment (STE) Installation and Use in Private Quarters

1. References:

a. AR 381-14, (U) Technical Surveillance Countermeasures (contains SECRET).

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

2. A secure telephone was installed in the private quarters of Colonel John M. Smith, Commander, 21st Sustainment Command (21st SC). Colonel Smith's quarters do not qualify for technical surveillance countermeasure support as defined in AR 381-14.

3. The STE is required in Colonel Smith's quarters for secure voice communications according to AR 380-5, chapter 6. Colonel 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 (about 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 STE will be installed at Flieger Street 58, Sherman Circle, George Washington Village, 67657 Kaiserslautern. The STE 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, 21st SC, will provide logistic support for the (military or *Deutsche Telekom*) telephone line. DD Form 2056, with the top portion of the decal blacked out, will be attached to the STE.

6. The security manager for this STE is Mr. Smart at military 490-1234. Maintenance and trouble support will be provided by CW3 Jones at military 490-5678 or civilian 0671-609-9012 (outside duty hours).

7. The STE is keyed with Secret, residence only, voice key. *The security manager must enter one of the following statements:*

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

Classified information will not be stored at the residence.

8. The POC for the 21st SC is Mr. Smart, military 490-1234.

FOR THE COMMANDER:

MICHAEL G. ROGERS
Colonel, GS
Chief of Staff

Figure 3. Sample Memorandum Confirming STE Installation in Private Quarters

SECURE TELEPHONE CERTIFICATION/RECERTIFICATION RESIDENCE INSPECTION CHECKLIST UNIT/ACTIVITY:	DATE:

Grade/Name:

Residence Address:

ITEM DESCRIPTION:	**YES**	**NO**
1. Equipment Identification:		
a. Type of secure telephone:		
b. Serial number(s):		
2. Documentation:		
a. Is a certification for secure-telephone installation in private quarters on file? Date:		
b. Is the secure-telephone approval on file? Date:		
c. Is the secure-telephone approval current?		
d. Does the user have the appropriate security clearance, and is the user certified by the loca commander as having responsibilities involving national security (AE Reg 380-40, para 11a(5)(f))?		
3. Markings:		
a. Is a U.S. GOVERNMENT PROPERTY decal applied to the front of the telephone (AE Reg 380-40, para 11a(5)(e))?		
b. Is DD Form 2056 applied to the front of the secure telephone (AE Reg 380-40, para 11a(5)(g))?		
c. Is an EMERGENCY NUMBERS decal applied to the instrument?		
d. Is a DO NOT REMOVE CARD WHILE OFF HOOK OR IN A CALL decal applied to the front of the instrument (STE only)?		
4. General:		
a. Is the secure telephone used as a standard telephone (AE Reg 380-40, para 11a(5)(a)1)?		
b. Is the secure telephone used for voice communications (AE Reg 380-40, para 11a(5)(d))?		
c. Do audio and physical-security precautions prevent unauthorized access to the secure telephone and KSV-21 card and prevent the interception of information (AE Reg 380-40, para 11a(5)(a))?		
d. Does the user know the numbers to call for a key update to the STE (mil 312-238-4470, civ 99-001-410-526-3470, toll-free 99-800-816-7980)?		
5. STE Operations:		
a. Is the KSV-21 card removed from the STE after each use (AE Reg 380-40, para 11a(5)(h))?		
b. Is the KSV-21 card controlled by the user or left in the custody of an authorized person (AE Reg 380-40, para 11a(5)(i))?		
c. Does the user know the procedures for protecting the KSV-21 card when it is not inserted in the STE? (TB 380-41)		
d. Does the user know the actions required if a KSV-21 card is lost (AR 380-40, chap 6)?		
6. Remarks:		

Certified Name: _____ Signature: _____

Figure 4. Secure Telephone Certification/Recertification, Residence Inspection Checklist

(c) The requester and the unit security manager will keep a copy of the approval on file.

(d) Unit security managers will notify the Security Branch, Office of the Deputy Chief of Staff, G2, HQ USAREUR, when the STE is no longer required and provide disposition instructions for turning in the KSV-21 or the GSM to the COMSEC manager.

(e) STE certified for use in private quarters is only for voice communications. Information discussed over an STE with a private resident will be no higher than Secret or its non-U.S. equivalent.

(f) 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.

(g) The user of the STE 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 KSV-21 card on AE Form 380-40D.

(h) The user will attach DD Form 2056 to the STE. If the quarters are cleared for classified discussions, the user will cut off the top part of the label that states *DO NOT DISCUSS CLASSIFIED INFORMATION* before affixing the label to the STE.

(i) The KSV-21 card must be removed from the STE after each use.

(j) The KSV-21 card must be controlled by the user or left in the custody of a cleared, authorized person. DOD security standards define "authorized persons" and prescribe controls.

(k) Users must be familiar with and maintain copies of DOD security procedures.

b. Timeport 280 (Secure Cell Phone) With a Secure Module (SM). The following standards and conditions must be met when using secure cell phones:

(1) Secure cell phones must be strictly controlled while in a private residence.

(2) Secure cell phones may be keyed to a level no higher than Secret.

(3) Only authorized persons will be allowed access to keyed secure cell phones.

(4) To prevent unauthorized use or loss, the SM must be physically separated from the cell phone when not in use, and the SM personal identification number (PIN) must be disabled. The SM must be in the user's personal possession or stored in a locked cabinet or drawer in an area separate from the cell phone.

(5) Secure cell phones will not be used to discuss classified information when uncleared personnel are present.

(6) Secure cell phones may be used only in residences that have been cleared for classified discussions. The room where the secure cell phone is used must have a lockable door, and the door must be closed and locked during classified discussions.

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

(8) Unusual incidents involving the residence of the cell-phone holder and the loss of a cell phone or an SM must be reported within 24 hours to the Regional Computer Emergency Response Team-Europe and to the unit—

(a) COMSEC manager.

(b) Information assurance support officer (IASO).

(c) Security manager.

(d) PBO or supply specialist.

(e) Telephone control officer.

(9) When no longer needed, the Timeport 280 must be turned off and returned with the SM to the primary hand-receipt holder (HRH) or the unit PBO. This must be done before moving from the residence, when the residence will be unoccupied for 2 weeks or longer, and before a permanent change of station or expiration term of service. The COMSEC manager, IASO, or security manager must be notified when the Timeport 280 and the SM are returned to the primary HRH or unit PBO.

12. SECTÈRA TIMEPORT 280 GSM CELL PHONE

a. Users of the Sectèra Timeport 280 GSM cell phone will detach the SM from the cell phone and place it in their pocket whenever they enter an area where cell phones are not authorized (for example, sensitive compartmented information facilities, secure workareas). The cell phone (without the SM) may then be placed into the cell-phone holding container (box) before entering the area.

b. The loss of a GSM-SM is a reportable COMSEC incident and must be orally reported to the COMSEC manager 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 HRH, COMSEC manager, and unit PBO. The statement must include the following:

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

(2) User’s full name, grade, and the last four digits of the user’s Social Security number.

(3) Unit or activity name (including division and branch, as applicable).

(4) The SN of the SM.

(5) Incident description. This must include—

(a) The date, time, and place where the loss was discovered.

(b) A complete description that explains that an SM was lost, who lost it, and when, where, why, and how it was lost.

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

c. Users of a Timeport 280 with a GSM-SM will sign a user agreement before using the cell phone (fig 5). Users authorized to use a Timeport 280 with a GSM-SM in a private residence will sign an acknowledgment of compliance with security procedures (fig 6). When users are away from their residence and do not have the cell phone with them, they must ensure the SM is detached and stored in a locked drawer away from the cell phone.

USER AGREEMENT ON THE USE OF A TIMEPORT 280 WITH A GSM SECURITY MODULE (GSM-SM)

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

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

2. The personal identification number (PIN) will not be affixed to the Timeport 280, GSM-SM, or any carrying cases for these devices. It must be kept in a location separate from the cell phone.

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

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

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

6. Any room where the Timeport 280 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 classified discussions.

8. If I lose a keyed Timeport 280, I will report the loss to the primary hand-receipt holder (HRH), communications security (COMSEC) manager, and unit property book officer (PBO) immediately (within 12 hours). Security incidents involving an unkeyed Timeport 280 must be reported to the primary HRH, COMSEC manager, and unit PBO within 24 hours.

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

_____ (Date)

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

Figure 5. User Agreement on the Use of a Timeport 280 With a GSM Security Module

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

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

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

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

3. The Timeport 280 with a GSM-SM installed will be keyed to a level no higher than Secret.

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

5. When the Timeport 280 is used to discuss unclassified information, the user will not discuss any classified information.

6. Only authorized persons will be allowed access to a keyed Timeport 280 with a 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 280.

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

9. The room in which the Timeport 280 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 classified discussions.

11. I will report any unusual incidents involving my residence, loss of the Timeport 280, or loss of the GSM-SM to the primary hand-receipt holder (HRH), communications security (COMSEC) manager, and unit property book officer (PBO) within 24 hours. The COMSEC manager will contact the information assurance support officer or information assurance manager.

12. I will ensure the Timeport 280 and the GSM-SM are returned to the COMSEC primary HRH when I no longer need them.

_____ (Date)

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

Figure 6. Acknowledgment of Security Procedures for Using a Timeport 280 With a GSM Security Module in Private Quarters

13. RELEASE OF CCIs

a. Requests for releasing CCIs will be made in accordance with AR 380-40, paragraph 8-4, and addressed through the USAREUR G2 (AEIN-IS), Unit 29351, APO AE 09014-9351, to the Director, Communications Security Logistics Activity (AMSEL-LCA-IAD), Fort Huachuca, AZ 85613-7041.

b. Questions about the release of CCIs in the European theater will be directed to the Security Branch, Office of the Deputy Chief of Staff, G2, HQ USAREUR (mil 537-2104).

14. CRYPTOGRAPHIC ACCESS PROGRAM

The unit security manager will be the CAP POC. Security mangers will coordinate with the unit COMSEC manager for a list of personnel who have access to Secret and TS keys. The CAP also applies to cryptographic maintenance, engineering, and installation technicians, regardless of their clearance, who meet all maintenance qualifications of AR 25-12 and have access to all maintenance manuals that include cryptologic information. Unit security managers will brief personnel on their responsibilities regarding the granted access and may revoke access in accordance with AR 380-40, chapter 7. Unit security managers will maintain a database of enrolled personnel.

15. COMSEC SUPPORT FOR COMSEC MATERIAL HAND-RECEIPT HOLDERS

A memorandum on COMSEC support for a COMSEC material HRH establishes an informal agreement between a unit commander (supported activity) who wants COMSEC support but does not have the personnel or financial resources and a unit commander who has a COMSEC account and will provide COMSEC support (supporting activity). Under the terms of an agreement, the most important responsibility for the supporting and supported activities is to provide the COMSEC material requested or required. Special consideration must be given when establishing an agreement between tactical and nontactical activities. All parties must understand their responsibilities before signing the agreement. Figure 7 is a sample agreement.

16. PROCEDURES FOR LOADING COMSEC ONTO NATO AND PARTNER-NATION END CRYPTOGRAPHIC UNIT DEVICES

a. All of the following conditions must be met before COMSEC material can be loaded onto a NATO or partner-nation end cryptographic unit (ECU) device:

(1) The COMSEC material must be releasable to the country.

(2) The CONAUTH of the keying material must authorize filling of a NATO Ally or partner nation ECU device by U.S. personnel.

(3) The device to be loaded must be a Type 1 encryption device.

(4) The country’s fill device must have become corrupt or subject to battery failure.

b. Keying material will not be issued to storage devices (for example, Simple Key Loader, Data Transfer Device).

c. All end devices filled by U.S. personnel will be tracked by SN. At the end of an exercise, all tracked radios will be personally verified as zeroed by a U.S. citizen. If possible, this should be the same person who filled the device.

d. A memorandum documenting the intent to load a NATO or partner-nation ECU must be completed and retained with the U.S. local element records at the supporting COMSEC account. The memorandum will address the following items:

(1) Country and unit.

(2) Reason for the request:

(a) Corruption of the database on the fill-device.

(b) Fill-device battery failure.

(3) Fill-device model and SN.

(4) ECU model and SN.

(5) Senior officer requesting the COMSEC key.

(6) USAREUR unit and local element.

NOTE: The memorandum in subparagraph d above will be used whenever key is loaded onto a foreign country's ECU device. The key will be given only to countries that have been specifically authorized by the CONAUTH (the owner of the key) and the unit's parent COMSEC account manager. The memorandum will be filed with the local unit's records along with the electronic key-management worksheet for 1 year from the date of filling the device.

COMMUNICATIONS SECURITY (COMSEC) SUPPORT AGREEMENT BETWEEN *Supported Activity* AND *Supporting Activity*

COMSEC SUPPORT FOR A COMSEC MATERIAL HAND-RECEIPT HOLDER

1. PURPOSE. This COMSEC support agreement between the *supported activity* and the *supporting activity* identifies resources involved and prescribes responsibilities of each signatory for COMSEC material hand-receipt support. This agreement is a mutual commitment to ensure COMSEC material is issued by the *supporting activity* as COMSEC manager on a hand-receipt to the *supported activity* and, once received, the COMSEC material is properly stored when not in use by appropriately cleared authorized persons and accounted for as prescribed in policy and procedures applicable to the material involved.

2. REFERENCES.

a. AR 380-40, Safeguarding and Controlling Communications Security Material.

b. TB 380-41, Procedures for Safeguarding, Accounting, and Supply Control of COMSEC Material.

c. AE Regulation 380-40, Safeguarding and Controlling Communications Security Material.

d. (*Other appropriate references.*)

3. BACKGROUND.

a. Army elements authorized COMSEC material normally obtain direct support by establishing a COMSEC account according to TB 380-41. When establishing a COMSEC account, the commander must select and appoint a COMSEC manager and at least one alternate manager. To ensure that two-person integrity can be maintained at all times, a manager and at least three alternates must be appointed for all COMSEC accounts that are approved for Top Secret material. Once appointed, the manager is responsible for safeguarding, controlling, and accounting for COMSEC material. COMSEC accounts are subject to various inspections, audits, and inventories.

b. The amount and type of COMSEC support required and personnel available may make establishing a COMSEC account impracticable or economically impossible. An alternative to establishing a COMSEC account is to obtain required COMSEC material that is on the hand-receipt of an established COMSEC account, preferably one within the same chain of command. Hand-receipt holders (HRHs) must safeguard, control, and account for COMSEC material in their care. COMSEC material HRHs have fewer and less time-consuming responsibilities than COMSEC managers.

c. Prompt compliance with established policy and procedures and cooperation between the manager and the HRH are essential for long-term support.

4. SCOPE. This implements the agreement for the *supporting activity* to issue COMSEC material to the *supported activity*.

5. RESPONSIBILITIES.

a. The *supporting activity* will—

(1) Provide COMSEC material support for HRHs on request.

Figure 7. Sample Agreement on COMSEC Support for a COMSEC Material Hand-Receipt Holder

(2) Conduct oversight visits to the *supporting activity* as required to ensure the HRH is properly using, safeguarding, controlling, and accounting for COMSEC material in accordance with AR 380-40, TB 380-41, and AE Regulation 380-40.

(3) Issue guidance (including SOPs) and provide advice and assistance as required to the HRH.

(4) Hand-receipt COMSEC material only to persons designated by the supported commander or responsible official.

(5) Notify the supported commander or other responsible official at the supported command when conditions or circumstances require attention.

(6) Provide the supported commander written notification at least 60 days before termination of a hand-receipt.

b. The *supported activity* will—

(1) Provide a current list of required COMSEC material to the *supporting activity*.

(2) Comply with Army policy and procedures and *supporting activity* SOPs applicable to using, safeguarding, controlling, and accounting for COMSEC material.

(3) Provide the *supporting activity* a list of cleared personnel authorized to sign for COMSEC material under this agreement and update this list as required to keep it current.

(4) Establish written procedures to ensure HRHs clear their hand-receipts with the *supporting activity* before permanent change of station or reassignment to other duties.

(5) Promptly notify the *supporting activity* when COMSEC material is lost, out of control, misused, or otherwise subjected to a possible insecurity.

(6) Be prepared to establish an organic COMSEC account or to begin receiving COMSEC support from an alternate source within 60 days after receipt of written notification from the *supporting activity* stating that COMSEC hand-receipt support under this agreement will be terminated.

6. REVIEW AND REVISION.

a. This agreement will be reviewed each year. The *supporting activity* will initiate this review within 90 days after the first year that the agreement has been in effect.

b. Either activity may propose a revision of this agreement at any time. Additionally, the agreement will be amended as necessary to comply with regulatory changes or changes in mission needs of either party.

7. EFFECTIVE DATE AND TERMINATION. This agreement will become effective on the date signed by the Commander, *supporting activity*, and the Commander, *supported activity*, and will remain in effect for 3 years unless extended or terminated.

_____[**signature**]_____	_____[**signature**]_____
(signature block of the supporting activity commander)	(signature block of the supported activity commander)
_____[**date**]_____	_____[**date**]_____

Figure 7. Sample Agreement on COMSEC Support for a COMSEC Material Hand-Receipt Holder—Continued

APPENDIX A
REFERENCES

SECTION I
PUBLICATIONS

CJCSI 3260.01C, (S) Joint Policy Governing Positive Control Material and Devices

AR 25-2, Information Assurance

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

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 190-45, Law Enforcement Reporting

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

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

AR 380-40, Safeguarding and Controlling Communications Security Material

AR 381-14, (U) Technical Surveillance Countermeasures (contains SECRET)

AR 710-2, Supply Policy Below the National Level

AR 710-3, Inventory Management Asset and Transaction Reporting System

AR 725-50, Requisitioning, Receipt, and Issue System

AR 735-5, Property Accountability Policies

DA Pamphlet 25-1-1, Army Information Technology Implementation Instructions

Technical Bulletin 380-41, Procedures for Safeguarding, Accounting, and Supply Control of COMSEC Material

AE Regulation 190-13, Army in Europe Physical Security Program

AE Regulation 350-1, Training and Leader Development in Europe

AE Regulation 380-85, Technical Security

AE Regulation 604-1, Local National Screening Program in Germany

Operational Security Doctrine for the KSV-21 Enhanced Crypto Card (ECC) and Secure Telephone Equipment (STE), DOC-007-07

Interim Operational Systems Security Doctrine for the GSM Security Module (GSM-SM) Operation With Timeport 280 Series Handsets

SECTION II
FORMS

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

DD Form 2056, Telephone Monitoring Notification Decal

DD Form 2501, Courier Authorization Card

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

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

DA Form 3964, Classified Document Accountability Record

AE Form 380-40D, KSV-21 Card Control Roster and Quarterly Possession Inventory

AE Form 380-40F, COMSEC Account - Local Daily Shift Inventory

APPENDIX B
SECURE TERMINAL EQUIPMENT PROGRAM GUIDANCE

B-1. PURPOSE

This appendix provides guidance on the Secure Terminal Equipment (STE) Program in the European theater. More information concerning STE (for example, user manual, software upgrades) is available at *https://cryptomod.kc.us.army.mil/*.

B-2. SECURITY

a. When requesting keying material, the location of the STE and the physical security measures in effect must be considered. The STE and KSV-21 card have been approved to protect classified information, including Top Secret and sensitive compartmented information (SCI). Access to SCI-level information is authorized only in sensitive compartmented information facilities.

b. The STE user and the area security manager must prevent unauthorized access to sensitive information. When a KSV-21 card is inserted in the associated STE, the system is considered to be unlocked, granting the user access to classified information. The system must never be left unattended unless it is in an area cleared for open storage of material of that classification level.

c. Commanders will designate a responsible individual to be the terminal privilege authority (TPA). The TPA will be responsible for configuring STE security features, upgrading the terminal's software, and inspecting the terminal's physical integrity. Commanders should assign the TPA as low in their organization as possible.

d. Communications security (COMSEC) managers will hand-receipt KSV-21 cards to an appointed TPA or card privilege authority (CPA) and authorize them to sub-hand receipt cards to end users.

(1) In some cases, such as in units or directorates with several STEs, COMSEC managers may sub-sub-hand receipt cards to users in their area of responsibility. This control will reduce the amount of paperwork and accounting required by the COMSEC manager.

(2) COMSEC managers are not required to physically inventory each card for semiannual inventory reports or change-of-manager inventory reports. Instead, COMSEC managers with large quantities of cards may verify the KSV-21 cards on hand by directing the TPA or CPA to physically inventory and certify a written inventory list of KSV-21 cards by serial number each quarter using AE Form 380-40D. This inventory will be called the quarterly possession inventory.

e. When KSV-21 cards are to be transported or shipped, COMSEC managers will not pack them in the same container with their associated STE. When using civilian carriers, COMSEC managers will ship KSV-21 cards by a carrier or mode separate from that used to ship the associated STE. If the same civilian carrier must be used because of urgent operational requirements, COMSEC managers will ship KSV-21 cards on a different day than their associated STE.

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

(1) Loss of a KSV-21 fill card.

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

(3) Known or suspected tampering of KSV-21 cards.

(4) Loss of a KSV-21 user card and associated STE.

(5) Loss of a KSV-21 user card and an associated KSV-21 carry card containing the other half of the KSV-21 user card key split.

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

g. Reportable administrative incidents include damage to or destruction, loss, or theft of a KSV-21 user card.

NOTE: STE is not a controlled cryptographic item (CCI). COMSEC managers do not account for CCIs. STE is handled and accounted for under the standard logistic supply policy. STE has tamper seals that the TPA will inspect in accordance with local logistic (that is, property book officer) policy. If tampering of 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 must be reported to the Security Branch, Office of the Deputy Chief of Staff, G2, HQ USAREUR. The TPA will observe and inspect the STE whenever a KSV-21 card is inserted.

h. KSV-21 cards are accountable under accounting legend code 1 and the Communications Security Material Control System, but they are not considered COMSEC keys. KSV-21 cards are not required and will not be included on a COMSEC account's DA Form 2653-R. KSV-21 cards can be inventoried and logged on AE Form 380-40F. AE Form 380-40F is a nonauditable form and kept separate from the consolidated DA Form 2653-R. AE Form 380-40F will be an item of interest during USAREUR command COMSEC inspections.

APPENDIX C
COMSEC ACCOUNT MANAGERS COURSE AND LOCAL COMSEC MANAGEMENT SOFTWARE COURSE

C-1. QUOTAS

a. Communications security (COMSEC) managers and command COMSEC inspectors must be graduates of the COMSEC Account Managers Course (CAM) and the Local COMSEC Management Software (LCMS) Course (AR 380-40). In the European theater, no person may be appointed on a COMSEC registration packet as a manager, primary alternate manager, or command COMSEC inspector without successful completion of the CAM and LCMS Courses. In European theater, the CAM is titled INT 34, and the LCMS is titled INT 35. INT 34 and INT 35 are offered by the Combined Arms Training Center (CATC) at Rose Barracks, Vilseck, Germany (*http://www.eur.army.mil/jmtc/CATC.html*). The CATC allocates quotas for the courses annually to commands in the European theater with a need to train personnel as COMSEC managers, alternate managers, or command COMSEC inspectors. Commanders who need more than their allocated quotas must send requests for authorization to attend a course through command channels to the USAREUR G2 (AEIN-IS), Unit 29351, APO AE 09014-9351.

b. Commands in the European theater will coordinate course quotas with the Schools Section, CATC.

C-2. PREREQUISITES

a. To attend INT 34, personnel must be enrolled in the Army Training Requirements and Resources System (ATRRS) and—

(1) Have no less than a “Secret” security clearance. This requirement is nonwaiverable.

(2) Have a memorandum signed by the unit security manager validating their security clearance.

(3) Have at least 1 year remaining in command after graduation (9 months for short-tour areas).

(4) Have a minimum grade of sergeant (E5) or GS-5.

(5) Be a candidate for a COMSEC manager, alternate manager, or command inspector position.

b. To attend INT 35, personnel must be enrolled in ATRRS and—

(1) Be a graduate of the CAM Course.

(2) Have a memorandum signed by the unit security manager validating their security clearance.

NOTE: Students arriving at the INT 34 or 35 course without the memorandum validating their security clearance will be sent back to their units.

C-3. WAIVERS

a. Requests for waivers to grade prerequisites must be sent through command channels to the USAREUR G2 (AEIN-IS), Unit 29351, APO AE 09014-9351. Requests must include—

(1) Name, grade, and Social Security number of the prospective student.

(2) Date expected to return from overseas (DEROS).

(3) Duty position.

(4) Class date and course number.

NOTE: Students enroll in CATC courses through ATRRS. Within 45 days before the course start date, all unreserved seats become available for fill by all commands. Even if a course is filled, a student may be entered into the system in a wait status. If a seat becomes available, the student in wait status will receive that seat. If no current information is available, the Schools Section, CATC, should be contacted at military 476-2849 or civilian 09662-83-2849 for a course number.

(5) Justification and verification of other prerequisites that are met.

b. Grade waivers to attend INT 34 or INT 35 are not approvals for appointment of those people to alternate COMSEC manager positions. Soldiers in grades below E5 and civilians in grades below GS-5 will not be appointed as alternate COMSEC managers nor be listed on the COMSEC account registration packet.

C-4. EMERGENCY ALLOCATIONS

Requests for emergency allocations for INT 34 must include the information in paragraph C-3a and be submitted through command channels to the USAREUR G2 (AEIN-IS), Unit 29351, APO AE 09014-9351.

a. Emergency allocations may be requested if unforeseen circumstances result in the loss of a COMSEC manager (for example, emergency leave, relief for cause).

b. Commanders will verify requests for emergency allocations and coordinate requests with training personnel to ensure that course quotas allocated in ATRRS have been filled by authorized candidates before sending the emergency request to the USAREUR G2.

GLOSSARY

21st SC	21st Sustainment Command
AE	Army in Europe
ALC	accounting legend code
AR	Army regulation
ATRRS	Army Training Requirements and Resources System
CAM	Communications Security Account Managers [Course]
CCI	controlled cryptographic item
CJCSI	Chairman of the Joint Chiefs of Staff instruction
COMSEC	communications security
CONAUTH	controlling authority
COOP	continuity-of-operation plan
CAP	Cryptographic Access Program
CATC	Combined Arms Training Center
civ	civilian
CPA	card privilege authority
CSLA	Communications Security Logistics Activity
DA	Department of the Army
DD	Defense Department
DLA	Defense Logistics Agency
DOD	Department of Defense
DODAAC	Department of Defense activity address code
G2	Deputy Chief of Staff, G2, United States Army Europe
G3/5/7	Deputy Chief of Staff, G3/5/7, United States Army Europe
G4	Deputy Chief of Staff, G4, United States Army Europe
G6	Deputy Chief of Staff, G6, United States Army Europe
GPS	Global Positioning System
GSM	Global System for Mobile Communication
GSM-SM	Global System for Mobile Communication - Security Module
HQDA	Headquarters, Department of the Army
HQ USAREUR	Headquarters, United States Army Europe
HRH	hand-receipt holder
IASO	information assurance support officer
LCMS	Local Communications Security Management System [Course]
mil	military
NATO	North Atlantic Treaty Organization
PBO	property book officer
PIN	personal identification number
SCI	sensitive compartmented information
SIPRNET	Secret Internet Protocol Router Network
SM	security module
SN	serial number
SOP	standing operating procedure
STE	secure terminal equipment
TB	technical bulletin
TLSC-E	Theater Logistics Support Center-Europe
TPA	terminal privilege authority
TS	Top Secret

TYAD	Tobyhanna Army Depot
U.S.	United States
USAFRICOM	United States Africa Command
USAREUR	United States Army Europe
USEUCOM	United States European Command