Army Regulation 380–40

Security

Safeguarding and Controlling Communications Security Material

Distribution Restriction Statement.
This publication contains technical or operational information that is for official Government use only. Distribution is limited to Government agencies or their contractors. Requests from outside the Government for release of this publication under the Freedom of Information Act will be referred to the Commanding General, U.S. Army Intelligence and Security Command, (IACSF–FI), Fort George G. Meade, MD 20755–5995. Requests from outside of the Government for release of this publication under the Foreign Military Sales program must be made to the Deputy Chief of Staff, G–2 (DAMI–CDS), 1000 Army Pentagon, Washington, DC 20310–1000.

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

Rapid Action Revision (RAR) Issue Date: 24 April 2013

Headquarters
Department of the Army
Washington, DC
9 July 2012

SUMMARY of CHANGE

AR 380–40
Safeguarding and Controlling Communications Security Material

This rapid action revision, dated 24 April 2013-

- Updates responsibilities for Commanding General, U.S. Army Intelligence and Security Command; Commanders, Army commands, Army service component commands, and direct reporting units; command security officers; commanders at all levels; and individual users (paras 1-8, 1-11, 1-12, 1-13, and 1-16).

- Provides expanded policy and guidance for administering the Counterintelligence Scope Polygraph Program in support of the Department of the Army Cryptographic Access Program (chap 7).

- Requires use of the U.S. Diplomatic Courier Service when shipping to foreign locations where controlled cryptographic items would be subject to foreign customs or postal inspection and clarifies the conditions and criteria under which controlled cryptographic items may be shipped using the Defense Courier Service mode of transportation (para 8-39).

- Makes administrative changes (throughout).

Headquarters
Department of the Army
Washington, DC
9 July 2012

*Army Regulation 380–40

Effective 9 August 2012

Security

Safeguarding and Controlling Communications Security Material

By Order of the Secretary of the Army:

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:

JOYCE E. MORROW
Administrative Assistant to the Secretary of the Army

History. This publication is a rapid action revision (RAR). This RAR is effective 24 May 2013. The portions affected by this RAR are listed in the summary of change.

Summary. This regulation prescribes Army policy for the safeguarding and controlling of communications security material. Also, this regulation implements National Security Directive 42, Executive Order 12333, the Committee on National Security Systems Policy Number 1, the Committee on National Security Systems Instruction 4005, DODI 5205.08, and portions of DODI 8523.01.

Applicability. This regulation applies to the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated. It also applies to non-Army elements that include, but are not limited to, contractors, consultants, and licensees. Its specific requirements apply to all communications security material in physical and electronic form used to secure national security systems. During mobilization or national emergency, the proponent may modify chapters and policies contained in this regulation.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff, G–2. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Army internal control process. This regulation contains internal control provisions in accordance with AR 11–2 and identifies key internal controls that must be evaluated (see appendix E).

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Deputy Chief of Staff, G–2 (DAMI–CDS), 1000 Army Pentagon, Washington, DC 20310–1000.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Headquarters, Department of the Army, Deputy Chief of Staff, G–2 (DAMI–CDS), 1000 Army Pentagon, Washington, DC 20310–1000.

Distribution. This regulation is available in electronic media only and is intended for command levels C, D, and E for the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

*This regulation supersedes AR 380–40, dated 30 June 2000. This edition publishes a rapid action revision.

Contents (Listed by paragraph and page number)

Contents—Continued

Contents—Continued

Contents—Continued

Contents—Continued

Figure List

Glossary

Chapter 1
Introduction

Section I
General

1–1. Purpose
This regulation prescribes the policy for safeguarding and controlling communications security (COMSEC) material in electronic and physical form and prescribes the Army security standards for implementation of the COMSEC Material Control System (CMCS). It supplements the policy, doctrine, directives, and instructions for COMSEC established by the Department of Defense (DOD), the National Security Agency (NSA), and the Committee on National Security Systems and authorizes the Headquarters, Department of the Army (HQDA), Deputy Chief of Staff, G–2 (DCS, G–2) to review, coordinate with the Chief Information Officer/G–6 (CIO/G–6), and distribute selected NSA doctrinal publications for Army use. Policy and procedures to implement supply control, item accounting, and transaction reporting for all COMSEC material are contained in technical bulletin (TB) 380–41, AR 710–2, AR 710–3, and AR 735–5.

1–2. References
Required and related publications and prescribed and referenced forms are listed in appendix A.

1–3. Explanation of abbreviations and terms
Abbreviations and special terms used in this regulation are explained in the glossary.

1–4. Responsibilities
Responsibilities are listed in section II of chapter 1.

Section II
Responsibilities
The ultimate responsibility for safeguarding COMSEC material rests with the individuals in possession of the material. This responsibility is inherent with the commander or comparable civilian director.

1–5. The Deputy Chief of Staff, G–2
The DCS, G–2 will—

a. Prescribe Army policy and approve procedures for safeguarding and controlling COMSEC material.

b. Coordinate with CIO/G–6 and the NSA, as appropriate, on the release of Army COMSEC material or foreign COMSEC material in custody of the Army to nonmilitary agencies, the general public, foreign nationals, or foreign governments.

c. Serve as the Army Staff representative to National and DOD working groups responsible for policy and procedures for safeguarding and controlling COMSEC material in support of the voting member for the Committee on National Security Systems (CNSS).

d. Manage the Department of the Army Cryptographic Access Program (DACAP).

e. Accept the cryptographic access granted by other DOD components.

f. Coordinate with the CIO/G–6 for the policy, development, dissemination, support, tactics, techniques, and procedures for the design, implementation, and operation of the key management infrastructure (KMI) and systems to support Army encryption requirements.

g. Develop policy and approve procedures for safeguarding and controlling of all COMSEC material, including controlled cryptographic items (CCIs).

h. Review and approve procedures for COMSEC logistics support.

i. Serve as the Army representative, with the CIO/G–6, for Army KMI security policy working groups.

j. Establish an Army COMSEC assessment program to evaluate compliance with DOD, Joint Staff, and Army policy and procedures. Assessment will include management effectiveness of COMSEC incident reporting, oversight of CCI accountability, currency and accuracy of the cryptographic access program, application of standardized COMSEC training, and general CMCS compliance.

k. Conduct semiannual oversight visits to the U.S. Army Communications Security Logistics Activity (USACSLA) to review Army COMSEC audit, inspection, and incident monitoring activity.

l. Ensure requirements of the CNSS as they apply to the DCS, G–2 responsibilities are met.

m. Manage Army responsibilities within the CMCS, including a central office of record and supported COMSEC accounts.

n. Establish procedures ensuring COMSEC account managers (CAMs) and alternate CAMs are properly appointed and trained and their clearances are verified.

o. Establish a protective technologies inspection program.

p. Ensure that all applicable policies, directives, criteria, standards, and doctrine relating to the safeguarding and controlling of COMSEC material are implemented within the Army.

1–6. The Chief Information Officer/G–6

The CIO/G–6 will—

a. Provide management oversight of the Army Key Management Enterprise Infrastructure, including implementation of the KMI, Electronic Key Management System (EKMS), and the Army Key Management System.

b. Provide an Army voting member to the Key Management Executive Committee and Joint KMI working group.

c. Provide information assurance (IA) guidance to Army elements in identifying and incorporating requirements consistent with the KMI requirements in project development as well as operations.

d. Serve as the principal Army member to the CNSS.

e. Appoint the chairperson and alternate chairperson for the Tier 1 System Management Board, which has operations management responsibilities for the EKMS Common Tier 1 System.

f. Implement procedural and material protective measures, develop plans and policies, and validate requirements to protect Army command, control, communications, and computers.

g. Review and validate all Army requirements for COMSEC products and services and forward validated COMSEC requirements to the Director, NSA as necessary to support procurement activities.

h. Appoint the Army approving authority for the Certification Authority Workstations (CAWs), which has operations management responsibility for the overall CAW security systems operations.

i. Promulgates rules and procedures in the Army certification practice statement outlining the certification authority, system administrator, and IA security officer responsibilities to keep Army CAWs operational and secure.

j. Review and approve Army key management plans.

1–7. Deputy Chief of Staff, G–4

The DCS, G–4 will—

a. Maintain serial number visibility over CCIs from procurement through demilitarization and disposal.

b. Provide oversight to ensure reporting of COMSEC CCI incidents as part of the Command Supply Discipline Program.

c. Establish an Army COMSEC CCI Assessment Program as part of the Command Supply Discipline Program to validate compliance with DOD, Joint Staff, and Army policy and procedures. Assessment will include management effectiveness of COMSEC CCI incident reporting and oversight of CCI accountability.

d. Prescribe and supervise the implementation of procedures for property control and the accounting of CCI material during distribution, storage, maintenance, use, and disposal. All guidance will conform to the security standards developed by the DCS, G–2 for safeguarding COMSEC material.

1–8. The Commanding General, U.S. Army Intelligence and Security Command

The CG, INSCOM will—

a. Assist commanders in making initial determination of whether formal assessment for foreign intelligence services involvement in COMSEC incidents is required.

b. As required by DODI 5205.08, plan, program, and budget resources to conduct random counterintelligence scope polygraph (CSP) screening examinations under the provisions of AR 381–20 and DODI 5210.91 in support of the DACAP.

c. Upon request, provide local commanders technical assistance in evaluating security-related issues and conducting risk assessments.

1–9. The Commanding General, U.S. Army Materiel Command

The CG, AMC, through the USACSLA will—

a. Operate and manage the Army's CMCS to include the Army COMSEC central office of record.

b. Develop and promulgate approved COMSEC accounting procedures.

c. Establish and close COMSEC accounts.

d. Maintain records of all COMSEC material issued to Army COMSEC accounts.

e. Maintain a comprehensive program that ensures Army COMSEC accounts are audited and inspected, including protective technology inspections.

f. Require controlling authorities review and validate their requirements for the cryptosystems and authentication systems under their control (Report Control Symbol GID–131, (Cryptosystems Evaluation Report)) annually.

g. Approve COMSEC account establishment.

h. Approve Army COMSEC facilities under the provisions of this regulation.

i. Provide technical assistance to Army COMSEC activities and non-Army elements maintaining Army COMSEC accounts.

j. Administer a COMSEC Auditor Certification Program for all COMSEC auditors and inspectors.

k. Administer a Command COMSEC Inspector Certification Course.

l. Serve as the Army COMSEC incident monitoring activity (see chap 6).

m. Ensure a semiannual review of the central office of record, incident, and audit operations are conducted and that key management is reviewed annually in accordance with AR 11–2.

n. Conduct formal audits and inspections of the Automated Message Handling System, Tactical Message System, and CAW.

o. Serve as approving authority for certification approval authorities.

p. Implement CMCS and KMI policy and procedures.

q. Serve as final adjudication authority and determine when reported COMSEC incidents result in COMSEC insecurities.

r. Ensure Army compliance with COMSEC access program requirements.

s. Provide standing membership on KMI working groups and the Common Tier 1 Joint Configuration Control Board.

t. Monitor in-transit shipments and transfers of COMSEC material within the CMCS to verify receipt.

u. Establish or approve accounting procedures for reporting receipt and transfers of COMSEC material.

v. Establish or approve accounting procedures for accounts under its cognizance.

w. Ensure compliance with accountability requirements for COMSEC material.

x. Establish inventory and audit procedures for COMSEC accounts.

y. Ensure audits are conducted in accordance with this regulation.

z. Provide CAMs relief from accountability.

aa. Through the U.S. Army Material Command Logistics Support Activity (LOGSA)—

(1) Manage the Department of the Army (DA) Central Registry for CCI.

(2) Operate and maintain the CCI Serialization Program (CCISP).

(3) Administer the assignment of management control numbers for commercial COMSEC products approved for local purchase by NSA and USACSLA.

1–10. Commanding General, U.S. Army Training and Doctrine Command

The CG, TRADOC will—

a. Develop and implement the COMSEC Account Managers Course (CAM Course), previously called the Standardized COMSEC Custodian Course, the Army Key Management System/Local COMSEC Management Software Course, and the CAW 5.X Course.

b. Provide a complete copy of the CAM Course, to include updates, to all Army commands (ACOMs), Army service component commands (ASCCs), and direct reporting units (DRUs) who conduct this training under authority from TRADOC and who comply with standards established by the Signal Center.

c. Authorize the release of all COMSEC training material to the Reserve Officers' Training Corps (ROTC).

d. Provide draft copies of all doctrinal concept of operations, field manuals, and other publications related to the safeguarding of COMSEC operations to the CIO/G–6 and the DCS, G–2 for review prior to publication or distribution.

1–11. Commanders of Army commands, Army service component commands, and direct reporting units

Commanders of ACOMs, ASCCs, and DRUs will—

a. Establish and maintain an aggressive command COMSEC inspection program in accordance with this regulation, ensuring all COMSEC accounts under their purview have received a command inspection at a minimum of once every 24 months. The commander will appoint the command COMSEC inspector. The command COMSEC inspector will be of sufficient rank or grade and possess adequate COMSEC expertise to effectively discharge assigned duties and responsibilities and meet the requirements listed in chapter 5 of this regulation.

b. Ensure the command security officer (G–2 or S–2) fulfills all the oversight responsibilities provided in paragraph 1–12.

1–12. Command Security Officers (G–2 or S–2)

The command security officer (G–2 or S–2) will—

a. Determine the appropriate level(s) below ACOMs, ASCCs, and DRUs at which command COMSEC inspectors are required.

b. Ensure each COMSEC account under their jurisdiction receives a command COMSEC inspection under the provisions of this regulation a minimum of once every 24 months.

c. Approve the transportation of key via U.S. flag carrier or foreign commercial aircraft outside the continental United States, except during unit deployments when prior approval is not required (see para 2–38 for details).

d. As directed by the Commander, implement the DACAP within their commands. The program may be managed at an ACOM, ASCC, or DRU level or decentralized down to the subordinate command level. (The Chief, National Guard Bureau may delegate this authority to the State and territory adjutants general.)

e. Control access to classified cryptographic information in accordance with chapter 7.

f. Carry out and administer a cryptographic access program. This program will include cryptographic access briefings, coordination with the Army Intelligence Polygraph and Credibility Assessment Program Manager (INSCOM) to ensure persons enrolled in the DACAP are subject to a random CSP, and execution of cryptographic access certificates (see Secretary of the Defense Form (SD Form 572 (Cryptographic Access Certification and Termination)).

g. Maintain records on all individuals who have been granted cryptographic access or have had their cryptographic access withdrawn. Arrange for retention of cryptographic access certificates or legally enforceable facsimiles in accordance with Army records disposition schedules.

h. Deny or withdraw cryptographic access to those individuals who fail to agree to, or comply with, the specific criteria identified in chapter 7, to include those enrolled in the DACAP who refuse to take a random CSP.

i. Incorporate this policy into appropriate training and awareness programs.

j. Annually, compile a list of all individuals within the command enrolled in the DACAP. This list will be used by the ACOM, ASCC, DRU, and the Army National Guard (ARNG) to randomly select five percent of the personnel on the list to take a CSP. The list of randomly selected individuals will be maintained by the command security office and submitted to the Army Intelligence and Credibility Assessment Manager to support the scheduling and conduct of the random CSPs.

1–13. Commanders at all levels

Commanders, who determine they need a COMSEC account will—

a. Appoint a CAM and at least one alternate CAM for each COMSEC account under their jurisdiction. In accounts that contain top secret COMSEC material, a CAM and at least 3 alternate CAMs will be appointed to maintain two-person integrity (TPI).

b. Ensure adequate resources are committed to the command's COMSEC program to ensure effective management and administration of COMSEC requirements.

c. Ensure that personnel appointed as CAMs successfully complete the TRADOC-approved CAM Course.

d. For automated COMSEC accounts, ensure that the CAM and primary alternate CAM successfully complete the TRADOC-approved Local COMSEC Management Software (LCMS) Course prior to appointment.

e. Ensure each COMSEC account under their jurisdiction receives a command COMSEC inspection a minimum of once every 24 months.

f. Establish and maintain an aggressive command COMSEC inspection program. Organizations that have no knowledgeable COMSEC personnel, except the CAMs and alternate CAMs, should make arrangements to use a qualified person from another organization within the same geographical area.

g. Ensure property book officers and users receive a command inspection of CCI records to ensure compliance with this regulation, AR 710–2, and AR 710–3 at intervals not to exceed 24 months as required by the command supply discipline program.

h. Implement the provisions of the DACAP within their command.

i. Identify those individuals who require cryptographic access and ensure they receive the cryptographic access briefing and sign SD Form 572, section I. In coordination with the ACOM, ASCC, DRU, or ARNG, as appropriate, ensure those individuals enrolled in the DACAP are subject to a random CSP as a requirement to maintain cryptographic access.

j. Deny cryptographic access to or withdraw cryptographic access from those individuals who fail to comply with any of the specific criteria identified in chapter 7, to include those who refuse to take a random CSP.

k. Ensure that designated managers perform internal controls reviews per AR 11–2.

l. Require the use of electronic keying and rekeying whenever possible.

m. Conduct mandatory risk assessments of all COMSEC facilities, storage areas, and other COMSEC operational areas per AR 190–51 and DA Pam 190–51.

n. Ensure all Soldiers and Army employees under their command (when performing the duties prescribed in this regulation) create and preserve the records required by this regulation. Ensure the command's records management official provides information and assistance in identifying the recordkeeping requirements of this publication or refer to the U.S. Army Records Management and Declassification Agency, if necessary.

o. Appoint a primary and alternate systems administrator for CAWs and ensure that administrators are trained and certified in accordance with AR 25–2 and meet the Information Assurance Technical (IAT) Level 1 requirement.

Note. (COMSEC account individuals exercising certain KMI roles on the KMI MGC will be required to meet similar IAT requirements as the current EKMS Tier 2 migrates to the KMI Management Client).

1–14. Directors of Headquarters, Department of the Army agencies and commanders of Army commands, installations, and activities

Directors of HQDA agencies and commanders of ACOMs, installations, and activities need to have knowledge of AR 340–21 and AR 25–55.

1–15. Communications security account manager

For the Active Army, the ARNG, the U.S. Army Reserve, and ROTC—

a. The CAM is the appointed person responsible to the commander or comparable civilian director for—

(1) Custody and accountability of CMCS centrally and locally accountable COMSEC material.

(2) Supervision and oversight of all hand receipt holders (HRHs) and local elements to ensure compliance with existing COMSEC material security, accounting, and operational policies and procedures.

(3) Acquisition, control, and distribution of all classified COMSEC material and cryptographic key in support of organizational missions.

(4) Serving as the designated user or administrator of EKMS.

(5) Advising the commander or comparable civilian director on all COMSEC-related issues.

(6) Performing other duties as described in TB 380–41.

b. When serving as system administrators or platform security administrators, CAMs must meet IA training and certification requirements for IAT Level 1 in accordance with AR 25–2 and DODD 8570.01.

1–16. Individual users

Individual users directly influence the effectiveness of protection available through cryptographic techniques and cryptographic systems, and are personally responsible for the following:

a. The physical protection and accountability of all COMSEC material in their possession or control.

b. Reporting to the proper authority any occurrence, circumstance, or act that could jeopardize the security or integrity of COMSEC material.

c. Complying with instructions provided by the CAM for safeguarding and controlling COMSEC material.

d. Complying with instructions provided by the property book officer (PBO) for safeguarding and controlling CCI equipment.

e. Individuals enrolled in the DACAP will agree to be subject to random CSP examinations and will attend such examinations when properly notified.

Chapter 2
Communications Security Material Control System

The CMCS is a logistics and accounting system used to safeguard and control COMSEC materials in a manner that assures their continued integrity, prevents access by unauthorized persons, and controls the spread of COMSEC materials, techniques, and technology when not in the best interest of the U.S. and its allies. The major components of the Army CMCS are the COMSEC central office of record, cryptologic depots, and the COMSEC accounts. COMSEC accounts can be manual or automated using the EKMS. In the near future, the KMI will replace the EKMS to manage Army COMSEC accounting and distribution requirements. These components implement control procedures for the transfer, storage, inventory, and disposition of CMCS accountable COMSEC material. COMSEC material includes items designed to secure or authenticate telecommunications. It can range from unclassified to top secret and includes hardware, electronic key, physical key, classified COMSEC equipment, CCIs, component parts, devices, documents, firmware, or software that embodies or describes cryptographic logic and other items that perform COMSEC functions.

2–1. Requirements for communications security material

A command must have a CAM, a COMSEC account, and an approved COMSEC facility to obtain COMSEC material. These 3 requirements are necessary to ensure COMSEC material is only transferred and received by properly cleared personnel with appropriate storage facilities.

2–2. Communications security account manager

A CAM and alternate CAM are appointed to manage the COMSEC requirements of a command or organization.

a. The CAM and alternate CAMs will be officers, warrant officers, enlisted Soldiers, or permanent civilian employees. The minimum rank or grade for the CAM is E–6, general schedule 7 or an equivalent grade from the defense civilian intelligence personnel system pay bands. The minimum rank or grade for the alternate CAM is E–5, general schedule 5, or an equivalent grade from the defense civilian intelligence personnel systems pay bands.

b. The CAM, alternate CAM, COMSEC clerks, and COMSEC equipment operators must be U.S. citizens and be cleared to the highest level of COMSEC material or key they can access.

c. COMSEC account personnel operating within the EKMS, using the COMSEC local management device (LMD) and/or key processor (KP) must have a minimum secret security clearance.

d. In addition, those individuals whose official duties require continuing access to unencrypted secret crypto or top secret crypto keying material are subject to the requirements of the DACAP described in chapter 7 of this regulation.

e. CAMs will have maximum retain ability, with a minimum of 1 year retention in the COMSEC account in long tour areas and 9 months retention in the COMSEC account in short tour areas to establish continuity and decrease the possibility of frequent replacement.

f. A CAM will be assigned to a defined and officially established Army Authorization Document System operational position within the organization. The CAM will not be assigned other collateral duties that would interfere with or detract from the duties and responsibilities of a CAM.

g. CAMs and alternates CAMs will be selected by the commanding officer (or the designated representative) or the civilian equivalent. In no case will the CAM or alternate CAM sign as the approving authority for the account registration packet or the COMSEC facility approval request.

h. Commanders O–6 or above (or civilian equivalent) in the chain of command are authorized to grant waivers to the grade restrictions for the CAM and alternate CAM on a case-by-case basis. The waiver must be signed by an officer O–6 or above in the chain of command (or civilian equivalent) and will be kept on file in the COMSEC account jacket file within the Army central office of record.

i. Contractors may be appointed as the CAM for COMSEC accounts designated as a "Contractor Maintenance COMSEC Account" only. All other CAMs are considered accountable officers who must be government officials.

j. Contractor employees will not be appointed as the CAM of an Army organizational COMSEC account.

k. All CAMs must satisfactorily complete the TRADOC-approved CAM Course prior to appointment. For manual accounts, the alternate CAM should also complete the CAM Course.

l. All automated Army COMSEC accounts must have at least 2 individuals (CAM and alternate CAM) who have successfully completed the TRADOC-approved LCMS Course and the TRADOC-approved CAM Course training prior to their appointment. In emergency cases, the ACOM, ASCC, or DRU commander may appoint an individual as the primary alternate CAM that has not received LCMS training; however, the training must be received within 3 months. The waiver signed by the ACOM, ASCC, or DRU commander, O–6 or above (or civilian equivalent), must accompany the new COMSEC account registration packet (CARP) appointing that individual as the alternate CAM.

m. A commander O–6 or above (or civilian equivalent) in the chain of command may, on a case-by-case basis, authorize the appointment of untrained personnel to fill a void created by the unplanned absence or departure of a CAM. However, the newly appointed CAM must be immediately enrolled and scheduled for training in Army Training Requirements and Resources System (https://www.atrrs.army.mil) and successfully complete the training within 3 months.

n. Individuals who fail to successfully complete the TRADOC-approved CAM Course or LCMS Course will not be appointed as a CAM or an alternate CAM.

o. The Army will accept formal LCMS training certificates issued by other DOD training institutions.

p. No individual will be appointed as a CAM over more than one Army COMSEC account at a time. Individuals may be temporarily appointed as alternate CAMs over no more than 2 Army COMSEC accounts, pending assignment of a permanent alternate CAM. In addition, the CAM will not be assigned duties that preclude sufficient time to accomplish CAM responsibilities.

q. Whenever the CAM will be absent for more than 60 consecutive days, all COMSEC material in the COMSEC account will be transferred to either the alternate CAM (provided the rank or grade and training requirements of this para are met) or to a newly appointed CAM. Automated accounts also require immediate access removal by the system administrator and termination of LCMS credentials assigned to the former CAM.

r. The appointment of a new (incoming) CAM terminates the appointment of the old (outgoing) CAM. However, the outgoing CAM remains accountable for all COMSEC material charged to the account until properly released by the central office of record. An outgoing CAM is considered properly released from COMSEC accountability when the central office of record receives the clearance for the incoming CAM.

Note. This does not provide relief from responsibility for loss of property accountability per AR 735–5.

s. When the CAM is allowed to depart prior to being released by the central office of record, the commander for whom the account is maintained assumes personal responsibility for all discrepancies in the account.

t. An inventory of COMSEC accountable material will be initiated within 24 hours after the unauthorized absence or sudden permanent departure of the CAM has been detected. The commander will assign one properly cleared witness to assist the alternate CAM in completing the inventory as soon as possible. The inventory will be conducted in accordance with TB 380–41. A new CAM will then be appointed. If either the alternate CAM or the cleared witness is subsequently appointed CAM, a change of CAM inventory is not required.

u. CAMs serving as system administrators or platform security administrators must meet IA training and certification requirements for IAT Level 1 in accordance with DODD 8570.01 and AR 25–2.

2–3. Communications security account manager duties and functions

The duties and responsibilities of a CAM include, but are not limited to, the following:

a. Ensuring all COMSEC material issued to, or generated and held by, the COMSEC account is safeguarded and controlled in accordance with the requirements of this regulation, TB 380–41, or the operational security doctrine for the associated COMSEC equipment or system.

b. Maintaining, preparing, and submitting the COMSEC account files accounting reports to the central office record.

c. Ensuring new or additional COMSEC material is properly requisitioned or generated.

d. Personally conducting or supervising the inventories required by this regulation.

e. Correcting any deficiencies involving procedures at the account.

f. Ensuring amendments to COMSEC publications are posted in a timely manner and residue pages resulting from page replacements are destroyed.

g. Ensuring all mandatory equipment hardware modifications are made to COMSEC equipment supported by the account (software upgrades are system administrator and user responsibility).

h. Ensuring COMSEC material is issued only to appropriately cleared or authorized individuals with approved storage facilities whose duties require it and briefing them of their responsibility for properly safeguarding and controlling the COMSEC material in their possession.

i. Maintaining records of all COMSEC material issued to users on hand receipts.

j. Initiating organizational procedures ensuring individuals do not leave the organization without first returning or destroying COMSEC material issued to them on a hand receipt.

k. Ensuring routine destruction of COMSEC material is accomplished in accordance with the requirements of this regulation and TB 380–41.

l. Ensuring standard operating procedure (SOP), emergency protection, or destruction plans exist at all COMSEC facilities (see glossary) served by the COMSEC account.

m. Ensuring COMSEC material handled within the CMCS is properly packaged for transportation and all received packages are examined for evidence of tampering.

n. Ensuring protective technologies are inspected in accordance with instructions published by the NSA Protective Technologies Division. All reports of tampering must be reported in accordance with this regulation.

o. Ensuring COMSEC material received or transferred by the account agrees with material listed on the accompanying transfer report.

p. Ensuring COMSEC incidents are reported in accordance with the requirements of this regulation and TB 380–41.

q. Making transportation arrangements and ensuring only authorized means are used for transporting COMSEC material.

r. Ensuring the COMSEC account holds only COMSEC mission essential material.

s. Providing users training in the proper procedures for safeguarding and controlling COMSEC material.

t. Working with the COMSEC user to ensure there is a continuing requirement for specific key or, if no requirement, recommending to the controlling authority (CONAUTH) or command authority that the account be dropped from distribution of that specific key.

u. Ensuring the account is properly transferred prior to departing an assignment.

v. Establish a continuity of operations plan (COOP) as part of the COMSEC SOP.

2–4. Communications security accounts

The corner stone for the protection and accountability of COMSEC material is the COMSEC account. Whether manual or an automated COMSEC account, there are 2 distinct types of Army COMSEC accounts to support field commands. They are described as follows:

a. The first and most common type of COMSEC account is one organic to an Army unit under modified table of organization and equipment (MTOE) or table of distribution and allowances (TDA) authorization documents per AR 71–32. Government employees must operate accounts organic to Army units. The CAM maintains a formal set of property accounting records that show, on a continuing basis, the item identification, gains and losses, on hand balances conditions, and locations for all property assigned to the account. The appointed CAM of this type of account must be a military or civilian Government employee and is designated an accountable officer, as defined in AR 735–5.

b. The second type of COMSEC account is operated by a Government contractor at a contractor facility. It is established to provide COMSEC maintenance services to ACOMs, and is designated a "Contractor Maintenance COMSEC account". This type of account is not organic to any Army unit. It may be provided Government facilities and government furnished equipment (GFE) under the terms of its contract, but the contractor must fund its own repair and operating cost. The contractor COMSEC account does not perform COMSEC distribution or operational functions and the COMSEC property maintained in the account is for internal use only or customer repairs. Government

contracts which require Army contractor accounts to receive CCI as GFE are authorized to account for CCI cryptographic devices in their COMSEC accounts. The accountability and responsibility for the COMSEC material is written into the contract. This eliminates the requirements to formally designate the contractor's CAM as an accountable officer. However, Army contractors may be held accountable, responsible, and pecuniary liable for U.S. Government property provided to them under the terms of their contracts (see the Federal Acquisition Regulation and the Army Federal Acquisition Regulation Supplement). Contractor personnel will not be designated as accountable officers, as defined by this regulation.

c. Any organization or activity that requires accountable COMSEC material must obtain such material through a COMSEC account. If an existing COMSEC account, either in the organization or activity or located in close geographic proximity thereto, cannot provide the support required, a new COMSEC account will be established. However, COMSEC accounts will be kept to a minimum consistent with operational and security requirements.

d. Except when otherwise directed by competent higher authority, deployable tactical combat brigades and other separate tactical organizations subject to deployment will establish and operate organic COMSEC accounts to support its operational missions.

e. Except as noted above for deployable tactical organizations, when an existing COMSEC account can adequately support the requirement for COMSEC material within a command or geographical area of operations, a new COMSEC account will not be established. The material will be provided to subordinate elements and users via hand receipt. When a commander determines that a hand receipt is not a viable method of providing support (for example, large volume of material is required), the responsible commander may request establishment of a separate COMSEC account.

f. If a COMSEC facility approval (CFA) for a HRH is determined to be required by the CAM, the local commander for the supporting COMSEC account will approve such HRH and user COMSEC facility. USACSLA approval of the HRH and user facilities is not required. However, such facilities are subject to inspection by command COMSEC inspectors and USACSLA auditors. The CAM is responsible for the training, briefing, and oversight of all HRHs.

g. The decision to establish either a HRH or a separate operational account is a command decision based on operational conditions.

2–5. Deployment of communications security accounts

a. Upon notification of a pending deployment, the commander of the deploying unit should coordinate with the ACOM, ASCC, or DRU G–2 and G–3 staff operations, and the combatant commander gaining command G–2 and G–3 to determine the operation conditions and assigned mission. This information is essential in assisting the deploying unit under finalizing its plans for deployment. Commanders must use this information to determine the availability and accessibility of COMSEC material to maintain required secure communications. Autonomous operations are directly dependent on availability of organic COMSEC assets and infrastructure. When a commander considers not taking organic COMSEC assets by making prior arrangements for COMSEC support from units in the projected deployment area, the following must be taken into account:

b. Who will be supported? (1) U.S. forces; (2) Allied; (3) Coalition; or (4) North Atlantic Treaty Organization.

c. Continuous COMSEC support at new station (for example, duration of support and duration of mission).

d. Need for COMSEC support at home station.

e. Length of deployment.

f. Requirement to support other units at the deployed locations.

g. Communications connectivity to Tier 1.

h. Accessibility of the supporting unit's COMSEC account.

i. Type of COMSEC material required for operations.

j. Systems, circuits, and types of secure communications required at new location.

k. Mission change while deployed.

2–6. Electronic Key Management System

The EKMS is composed of 4 different levels referred to as tiers.

a. Tier 0 is the management level at NSA.

b. Tier 1 is the management level at the Services.

c. Tier 2 is the management level at the COMSEC account.

d. Tier 3 is the user level management.

2–7. Electronic Key Management System communications security accounts

Below Tier 1, the EKMS consists of automated workstations using LCMS to manage COMSEC functions and requirements and to administer the COMSEC account. The LCMS workstation consists of a LMD and a KP, secure terminal equipment (STE), and key storage devices (data transfer device (DTD) or simple key loader (SKL)). The KP is a secret CMCS accountable cryptographic item of equipment. The LMD is a standard commercial computer that becomes classified secret when loaded with LCMS (software). EKMS has given the Army the tools to move away

from paper-based keying material (physical key) that is centrally produced and distributed throughout the world via the Defense Courier Service to electronic key, generated by the NSA central facility or locally using the LCMS workstation and distributed electronically to the user.

a. The LMD must be protected as secret equipment at all times. The LMD must never be left unattended while in a logged on state. Should the operator need to leave the LMD, they must log off of the LMD platform. For top secret accounts, if 2 operators are logged in, both must remain in the direct presence of the KP during the time they are both logged in to maintain the TPI rule.

b. Two appropriately cleared KP operators must be physically present when the KP is keyed to output unencrypted top secret key (2 CIKs have been inserted) or when outputting key designated as TPI. An operator who is authorized (privileged) top secret may use the KP in the secret mode without TPI. But, once the operator desires to output unencrypted top secret key, the TPI mode (2 operators present) must be entered and the KP must be considered top secret. The KP reverts to secret upon exiting from the TPI mode at system shutdown or zeroization of the KP. Also, TPI does not apply to processing of top secret benign key, which can be performed with only one operator since benign key is never in unencrypted form. When 2 operators are logged onto the KP (TPI-enabled), the LMD and/or KP and the immediate area around the terminal will be considered a "no-lone zone."

c. The EKMS workstations must be certified and accredited in accordance with AR 25–2 by the appropriate designated approving authority.

d. While in operation, the EKMS workstation must be under the direct control of the CAM or alternate CAM and requires the same security protection as does any other computer processing information classified at the same level.

e. The LMD and/or KP System, including connecting cables, must be located in an area where it will receive at least secret level protection during operation. Access to the LMD and/or KP System must be limited to CAMs, LMD, and/or KP system administrators and operators.

f. When not in operation the LMD/KP must be stored either in an area approved for open storage of at least secret material, or the LMD hard drive and KP must be stored in the General Services Administration (GSA)-approved security container. Access to the area or security container must be limited to CAMs and operators. All EKMS associated CIKs must be removed from the KP and be stored in the GSA-approved security container.

g. Accounts which are open storage must have the room or facility identified on the COMSEC facility approval for the account. For accounts in which the open storage of the LMD and/or KP (operational configuration) is essential, the USACSLA-approved COMSEC facility must meet either secure room or vault standards, as stated in appendix C of this regulation. For deployed accounts, the commander may deem additional security measures, such as, guards, access controls, and continuous manning, appropriate in lieu of the appendix D requirements.

h. In accounts where the COMSEC facility is a GSA-approved safe or series of safes, the KP must be disconnected from the workstations configuration and stored in the safe along with the LMD hard drive. Exception: When the LCMS workstation is operated in an approved secure room or vault approved for storage at the secret level and the only individuals granted access have a secret or higher security clearance, the LMD and/or KP may remain in its operational configuration; provided all operational CIKs and personal identification numbers (PINs) used to operate the LCMS work station are properly secured in a GSA-approved safe.

Note. Any evidence of tampering or attempted use of the LCMS workstation by unauthorized individuals must be reported as a COMSEC incident.

i. For top secret accounts, the re-initialization 1 and re-initialization 2 keys must be secured in a GSA-approved security container with access limited to top secret cleared personnel. TPI controls are not necessary. PINs must be stored separately from the disaster recovery kit.

j. Key generators (KG–83, KGX–93, and KGX–93A) generating operational key will either be stored in a GSA-approved security container or secured in its mounting by means of a hinged locking bar that is locked in place, on a TPI basis by two approved combination locks. TPI controls are not necessary, except when extracting top secret key from the generator.

2–8. Access to communications security material

The sensitivity of classified COMSEC material requires that strict need-to-know procedures be followed. No person is entitled access to classified COMSEC material solely on the basis of rank, office, position, or security clearance.

a. Access to classified COMSEC material may be granted to U.S. citizens whose duties require access. Security clearance requirements for persons granted access is determined by the classification level of the material to be accessed. Depending on the classification of the material accessed, DACAP briefing certification must be verified prior to granting access.

b. Interim clearances are acceptable for U.S. Government employees. Contractor personnel must comply with CNSS Policy No. 14, therefore a final security clearance is required.

c. Under the provisions of AR 380–67, only U.S. citizens are authorized a security clearance. Immigrant aliens and local national employees of the Government are not authorized access to classified cryptographic material. Immigrant aliens may have access only to unclassified key marked crypto when their duties require access. They may not be—

(1) Appointed CAMs or alternates CAMs.

(2) Given access to information concerning the development or production of key.

(3) Given access to research and development information pertaining to any COMSEC equipment.

d. Photographing classified COMSEC material is prohibited.

e. When official photographs of COMSEC equipment or CCI are required and authorized, the following guidelines must be followed:

(1) Requirement must be validated and approved by the commander or security officer.

(2) No photographic equipment may be taken into areas where keying material is exposed or visible.

(3) All keying material must be secured in a locked container and areas sanitized prior to photographic equipment being allowed into the area.

(4) No photographs of equipment interior may be taken. Official photographs of the equipment exterior may be taken. Official or unofficial photographs, drawings, or descriptive information for press releases or private use are prohibited.

f. No access requirements are imposed for external viewing of COMSEC equipment where no opportunity exists for unauthorized access to the key, the COMSEC equipment, or the input and output of the COMSEC System.

g. Requirements for access to CCI are addressed in chapter 8, except that foreign access to keyed CCI is allowed only when all of the following criteria are met:

(1) Such access is in connection with building maintenance, custodial duties, or other operational responsibilities.

(2) The CCI is installed within a facility that is a U.S. controlled facility or a combined facility with a permanent U.S. presence, as opposed to a host nation facility.

(3) The cognizant security authority has determined that the risk of tampering with the CCI, which could result in compromise of U.S. classified or sensitive unclassified information, is acceptable in light of the local threat, vulnerability, and sensitivity of the data being protected.

(4) The system doctrine for the specific CCI does not prohibit such access.

(5) The foreign national is a civilian employee of the Government or assigned to a combined facility.

(6) The CCI remains U.S. property and a U.S. citizen is held responsible for it.

(7) The presence of such installed CCI is verified at least monthly, although no reporting is required.

(8) The communications to be protected are determined to be essential to support U.S. or combined operations.

(9) U.S. personnel must be aware of the foreign national status of CCI users.

(10) Keying of the CCI with classified U.S. key must be done by U.S. personnel. Authorized foreign nationals may do keying of CCI with allied or unclassified U.S. key.

h. Clearances are not required for access to unclassified COMSEC material, which includes an encrypted key. Access to unencrypted key must be restricted to persons with an interim or final clearance at the appropriate level and a need-to-know. Individuals with access to unencrypted key must be properly briefed in accordance with this regulation regarding the sensitivity of the material, the rules for safeguarding such material, the laws pertaining to espionage, the procedures for reporting COMSEC incidents, and the rules pertaining to foreign contacts, visits, and travel (see app D).

i. Contractors and nongovernment persons acting under the direction of the U.S. Government may be granted access to COMSEC material and information within the provisions of CNSS Policy No. 14 and CNSS Policy No. 3.

j. Resident aliens who are Government civilian or military personnel may have access to unclassified COMSEC material if required to perform their duties. However, resident aliens may not be appointed as CAMs or have access to areas where COMSEC material is stored in a manner such that it could be viewed, copied, and transferred.

k. Foreign nationals who are representing a foreign government or international organization may be given access to COMSEC information that has been specifically released to the represented government or organization under the provisions of National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 8. Before any release is made, the foreign government or organization must state in writing that the representative has an appropriate clearance and is officially designated to receive the information.

l. Access to future editions of unencrypted keying material must be limited to COMSEC account personnel until the keying material is issued for use. When unencrypted key is stored electronically, system or procedural safeguards must be used to limit access to account personnel. Exceptions can be made to these access restrictions in tactical situations when mission requirements dictate.

m. Whenever possible, encrypted key (not derived from benign keying techniques) must be handled and stored separately from its associated unencrypted key encryption key (KEK) until it is loaded into the end crypto-unit or consuming device. If this is not possible, the encrypted key must be considered classified to the level of the underlying information. For procedures on specific equipment holding both the encrypted key and its associated KEK, see specific systems doctrine.

n. Release of COMSEC material to contractor personnel must be included on the DD Form 254 (Department of Defense Contract Security Classification Specification).

2–9. Accessing, viewing by, and releasing of communications security material to foreign nationals

a. Foreign students viewing COMSEC material as part of their training must be informed that such viewing does not imply COMSEC material will be released to their government.

b. The restriction on viewing COMSEC material does not apply to photographing of COMSEC material. Except as provided for in paragraph 2–8, all requests for photographing of COMSEC material will be forwarded to DCS, G–2 (DAMI–CDS).

c. Foreign nationals representing a foreign government or international organization may be given access to COMSEC information specifically released to the represented government or organization under the provision of NSTISSP No. 8 and Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.06B. Access is defined as the opportunity to make use of an information system resource.

d. NSTISSP No. 8 defines release as a deliberate review and decision process undertaken by the CNSS and national manager to share, either on a temporary or permanent basis, U.S. Government information security products or associated information security information with foreign governments or international organizations in satisfaction of U.S. Government foreign policy and military or economic objectives. All Army activities will comply with that policy. Request for access to COMSEC material by foreign nationals (equipment and information) must follow the instructions in CJCSI 6510.06B.

e. Unclassified COMSEC information obtained from open sources may be used in Army schools when foreign nationals are being trained. Open source information, for the purposes of this regulation, is public domain information, or any type of publicly available information (for example, government reports, commercial vendor information, and Internet searches). Information any member of the public could lawfully obtain by request or observation, without restriction, may be used in Army training environments. Open source information also includes any information that may be used in an unclassified context without compromising national security or intelligence sources and methods. If the information is not publicly available, certain legal requirements relating to collection, retention, and dissemination may apply.

2–10. Top secret communications security material

The proper handling of COMSEC material applies to all COMSEC material that is not in storage, loaded, or resident in an end cryptographic unit (ECU) or covered by destruction policy.

a. The top secret key is used to protect the most sensitive U.S. national security information. Its loss to an adversary can compromise all of the information protected by the key. There is a significant body of information indicating that top secret key is a high-priority target for exploitation by foreign intelligence services. For this reason, top secret key must be afforded special protection. TPI and no-lone zones are used to meet this requirement.

b. TPI means that the top secret key must always be in the possession of 2 appropriately cleared persons who are authorized access to the material. Hard copy (physical) top secret key still in its protective packaging (for example, canister) does not require TPI controls when outside a storage container (for example, safe and vault), provided the CAM and the alternate CAM, who has possession of the key is registered in the DACAP. However, when key is removed from its protective packaging (for example, a segment is removed from a canister) or when the protectively packaged key is hand receipted to a user, all material will be signed for by 2 appropriately cleared individuals and will be maintained under TPI controls. Requests for exception to TPI will be forwarded through command channels to DCS, G–2 (DAMI–CDS) for consideration.

2–11. Use of no-lone zones

a. A no-lone zone is an area, room, or space where no person will have unaccompanied access. A no-lone zone must always be occupied by 2 or more appropriately cleared people who can observe each other's actions.

b. No-lone zones will be established whenever top secret key can be accessed from COMSEC equipment, either in physical or electronic form (for example, facilities where electronic key is generated). No-lone zones are not required where the COMSEC equipment is installed in a manner to preclude access to the equipment for extraction of key. However, TPI controls will apply to all initial and rekeying operations using top secret key. Key distribution centers and key generation centers, communications security logistics support facilities (CLSFs), or other logistics activities that store, generate, or distribute top secret key are subject to no-lone zone restrictions. In addition, activities engaged in the design, development, training, or maintenance of COMSEC equipment should consider the application of no-lone zone restrictions.

c. No-lone zones will be specifically designated by the commander and a physical description of the no-lone zone will be posted within the area, room, or space that contains the no-lone zone.

d. Whenever 2 persons are logged onto the KOK–22A, TPI-enabled, the LMD and/or KP and the immediate surrounding area become a no-lone zone as defined in paragraphs *a* and *b*.

e. Requests for exception to the no-lone zone requirement will be forwarded through channels to the ACOM, ASCC, or DRU command security office for consideration on a case-by-case basis.

2–12. Communications security software, encrypted key, and JOSEKI

COMSEC software, as well as, any associated encrypted software must be handled and stored separately from the combination key splits or keys, which together provide the ability to decrypt the software. If this is not possible, the key and software must be considered classified to the level of the underlying information. Electronic key is considered to be stored separately if the key is unable to be viewed, copied, or transferred and the associated keys can only be joined with the encrypted software with proper authorization.

a. Keying material and software, which is encrypted via NSA-approved means, is considered unclassified and/or for official use only (FOUO) unless the operational systems security doctrine directs otherwise. Use of specific media or systems may necessitate additional safeguarding and control requirements.

b. Encrypted algorithms will not be marked crypto and may be handled outside the CMCS. Unencrypted (RED) key, which decrypts such data, will be controlled within the CMCS.

c. RED key includes unencrypted key and the controlled portions of split keys. At least one split of a key (for example, one JOSEKI split), which enables COMSEC software (including encrypted algorithms) to be decrypted and used must be considered RED key. Specific systems doctrine defines control requirements for each equipment and may differ from this general requirement.

d. KEKs, which encrypt keying material, must be handled in accordance with the classification of the information it is protecting, unless the systems security doctrine directs otherwise.

e. Likewise, at least one of the keys or splits used to encrypt or decrypt classified software (also known as a "package decryption key") must be handled in accordance with the classification of the information being protected, unless the operational system's security doctrine directs otherwise. JOSEKI (algorithm) splits or keying material associated with any software package protection mechanism ("package decryption keys") are considered to be keying material for control and access purposes. The key will be handled and controlled in the CMCS as a noncrypto accounting legend code (ALC) 6 item.

f. NSA will be responsible for the establishment of a central repository for the management and distribution of algorithms in encrypted form. NSA will also be responsible for ensuring the distribution of the associated decrypt splits (key).

g. JOSEKI is the name of an unclassified cryptographic algorithm, which is only used to encrypt and decrypt software algorithm implementations. JOSEKI is not the only such algorithm in use and other algorithms may be used for this same purpose in the future.

2–13. Dissemination of communications security material

a. All electronic and physical keying material, classified COMSEC equipment, and COMSEC publications assigned an account legend code by the NSA will be entered into the CMCS.

b. All CCI and other unclassified COMSEC hardware items will be entered into the standard Army supply system and logistically managed under AR 710–2, AR 725–50, and TB 380–41.

c. In DOD channels, COMSEC material (other than that specified in para *a*) may be distributed and accounted for in the same manner as other national security or national security-related information. Also, after initial receipt in the CMCS, classified COMSEC material not requiring central accounting may be distributed and accounted for under AR 380–5 or TB 380–41.

2–14. Minimum item accounting requirements

a. All keying material is under accounting controls throughout its life cycle, from the moment it is generated, and upon receipt, until final disposition through issue, transfer, or destruction. Accounting procedures are contained in TB 380–41. Tier 1 Army central office of record will maintain a record of all accountable COMSEC material issued to COMSEC accounts.

b. Key designated as centrally accountable will be continuously accounted for from time of receipt or generation through final disposition. A physical inventory of this key must be reconciled with the Army central office of record every 6 months. The Tier 1 is the automated accounting system the central office of record uses to perform key management and accounting functions. Semiannual inventories will be completed with the Tier 1 site that the COMSEC account is assigned to either Fort Huachuca, AZ or San Antonio, TX.

c. Key designated as locally accountable after receipt or generation and key designated not accountable after a specific time or event will be accounted for locally by COMSEC accounts until final disposition. These keys will be designated as ALC 4 or ALC 7.

d. Centrally accountable COMSEC material (ALC 1, 2, and 6) must be inventoried at least every 6 months and the inventory reconciled with the Army central office of record. Other locally accountable COMSEC material (ALC 4 and 7) must be inventoried at least annually and upon change of the CAM. CCI will be physically inventoried per AR 710–2 quarterly by HRHs and the results reported to accountable officers.

e. The standard form (SF) 153 (COMSEC Materiel Report), including those automated copies produced by EKMS, or other means, is the primary form used to perform most COMSEC material accounting transactions.

2–15. Reporting and accounting for communications security material

COMSEC material, other than that generated under the provisions of NAG–16, is assigned to 1 of 5 ALCs depending upon classification, purpose, and inventory requirements.

a. ALCs 1, 2, and 4 are assigned to physical material that must be inventoried ("sighted") by the CAM.

b. ALCs 6 and 7 are assigned to material in electronic form that cannot be physically inventoried but must be electronically inventoried by EKMS-certified (or otherwise NSA-approved) devices. EKMS and its successors may be used by the CAMs to maintain disposition records and support reporting requirements for all classes of material.

c. Tactical key generated under the provisions of NAG–16 is not assigned an ALC.

d. The Army may not reassign material to different ALCs without prior approval from NSA, except when such reassignment is an intrinsic part of an electronic key distribution process performed by EKMS (for example, see the LMD and/or KP and DTD specific doctrine for details).

2–16. Accounting legend code 6

ALC 6 material is continuously accountable to a central office of record by EKMS transaction and inventory reporting. NSA Central Facility generated and managed electronic key will be assigned ALC 6. Some examples of ALC 6 key are—

a. Electronic key intended to protect information having long-term intelligence value, where such determination is made by the CONAUTH (for example, top secret and sensitive compartmented information).

b. Electronic key (KEK) used to protect other keys when such keys are widely distributed (for example, out of the local area).

c. Electronic key used for Joint and combined interoperability when such keys are widely distributed.

d. Electronic key marked crypto used to generate other electronic key (for example, key production key).

e. Electronic JOSEKI noncrypto splits.

2–17. Generating and accounting for accounting legend code 6 material

a. A report will be submitted to the central office of record upon the generation, receipt, and all subsequent transfers of all ALC 6 material. The central office of record will maintain a record of all ALC 6 material charged to a COMSEC account. All transactions involving ALC 6 material including, but not limited to, issue for use and destruction (zeroization) will be recorded in a local disposition record. The local disposition records will be retained by the CAM in accordance with TB 380–41 until audited by USACSLA.

b. CMCS accountability is required to account for the JOSEKI private split. The system administrators are responsible for tracking the movement and use of encrypted software packages locally, in order to keep track of which software version is installed in each ECU. Local users and system administrators who load the splits into equipment are required to keep a record of which software version is installed.

2–18. Generating and accounting for accounting legend code 7 material

a. Key may only be sent to users with the CONAUTH's explicit permission. CONAUTHs must be able to document all users of their key. Each recipient of ALC 7 key will report receipt to the key management infrastructure element (for example, EKMS element) that sent the key. Accounts generating ALC 7 key must maintain local records, which document the generation of key and identify all recipients of the key. All holders of ALC 7 material must maintain local disposition records, which permit traceability to support compromise recovery and audits. As a minimum, these records will identify all transactions involving subsequent transfer, issue, fill, and destruction of the material.

b. ALC 7 material requires continuous local accountability within the EKMS. Locally generated and managed electronic key and other electronic data which must be managed within the CMCS and is not covered by ALC 6 accounting policies cited above, will be assigned as ALC 7 by the CAM.

c. Electronic keys and key splits used to protect software algorithms or software that performs cryptographic functions are ALC 6 or 7 material.

2–19. Inventory requirements

a. NSA will maintain a central repository of all authorized and available COMSEC software.

b. The Army will maintain a repository of COMSEC applicable software. A real-time current inventory of software loaded into individual equipment within an organization is required at the lowest levels.

c. Army system administrators for COMSEC equipment are responsible for tracking COMSEC equipment, determining the version of both software and hardware currently existing in the equipment, being aware of what upgrades are available, and applying upgrades to both software and hardware on a timely basis, as mandated by higher authority. Tracking of equipment requires that a database be maintained. Equipment may be marked or tagged with recognizable electronic identifiers so that the equipment is able to be interrogated directly to determine the current software and hardware configuration.

d. At user locations, physical keying material marked crypto will be inventoried by serial number on days when the security container is opened (containers do not need to be opened for inventory purposes only). The inventory will be

made a matter of record using DA Form 2653–R (COMSEC Account - Daily Shift Inventory). Other COMSEC material will be inventoried in accordance with the instructions of the central office of record.

2–20. Issuing

Key transferred electronically from one account to another will be recorded as such by the initiating CAM and receiving CAM. For key issued to a local element, the CAM should retain a hand receipt (or legally equivalent digital signature) that provides a basis of receipt, inventory, and reconciliation for key issued to a DTD or SKL. Alternate methods such as EKMS worksheets, SF 153, and locally developed disposition statements are also acceptable, provided all basic elements of information to maintain strict accountability are incorporated into the documentation.

2–21. Removable storage devices

If key is transferred as a bulk encrypted transaction from Tier 1 or from an LMD by means of a removable storage device the removable storage device must be classified secret (since these systems are secret high systems). The notice "COMSEC Accountable" will also be physically marked in bold type on the removable storage device to indicate the material must be tracked within the CMCS. The LMD may only issue encrypted key. Key may be transferred from Tier 0 at the unclassified level. An electronic SF 153 is included in the individual EKMS bulk-encrypted transactions on the disk, which may be composed of various short titles and editions.

a. Secret removable storage devices may be downgraded by using procedures approved in its operational security doctrine.

b. Unencrypted key distributed on a removable storage device by the NSA Central Facility or Army Tier 1 central office of record, is assigned ALC 6 if it originally came from Tier 0.

c. Secret magnetic media containing encrypted keying material may be shipped to the authorized user by any means approved for secret material. Once received, the media must be protected at the secret level. As soon as practical after receipt, removable storage devices from the EKMS system (containing bulk-encrypted transactions) must be loaded into the designated LMD and/or KP in order to verify the integrity of the data. The disks may then be destroyed, degaussed, or overwritten. It may be reused for EKMS purposes only or degaussed using NSA-approved methods. Backups of the disks will subsequently become part of the LMD and/or KP database backup.

d. EKMS removable storage devices should not be directly copied by the user, as they may not be used elsewhere. The contents of the floppy disks must be loaded into the LMD and/or KP because it is not possible to determine the contents of the floppy disk without decrypting the bulk-encrypted transactions.

e. Encrypted information on the disk can be treated as unclassified and/or FOUO. However, the floppy disk itself must be controlled as secret.

f. Media from an LMD and/or KP to another system such as Army Continuing Education System or data management device cannot be reintroduced into the EKMS LMD without being degaussed. If no NSA-authorized degaussing method is available, the CAM must use a new disk.

2–22. Using communications security material

a. COMSEC material will be used only for its intended purpose.

b. Automated information systems used in national security systems producing or storing unencrypted key or unencrypted algorithms in electronic form, must be either standalone systems or networks or systems in a network environment using protection mechanisms and devices that have been evaluated and approved for use by NSA.

2–23. Communications security operational precautions (safeguards)

When a commander or other responsible official in a nontactical environment is required to establish and operate COMSEC equipment to process up to secret information in a room or building not meeting the standards of appendix C, a permanently constructed facility providing a reasonable level of security and control may be used after receiving approval from the ACOM, ASCC, or DRU security office.

a. During operation of keyed COMSEC equipment the user must ensure both physical and electronic security countermeasures have been applied. Cleared guards or operators can provide the requisite physical security during operation and the use of TEMPEST countermeasures and technical surveillance countermeasures can reduce the probability of any electronic security issues.

b. Unattended operational COMSEC equipment requires additional measures to prevent unauthorized access to the equipment and its output. Whether in a military work site, office building, or the personal quarters of high-ranking officials, operational COMSEC equipment must be protected from unauthorized access. Depending on local risk assessments and existing conditions, this could entail the use of equipment locking bars, specially designed GSA-approved security containers, or high security padlocks.

c. For part-time operations, storage of equipment, when nonoperational, must follow the NSA-published Systems Operational Security Doctrine for the equipment in use. For CCI equipment, this could mean simply removing the CIK or token from the equipment and storing them separately from the equipment. Providing double barrier protection for the CCI equipment under such conditions is considered adequate.

d. The system must be installed and comply with AR 380–5, AR 380–27, and AR 381–14.

e. Nonstandard facilities will not be used at the top secret level unless approved by the ACOM, ASCC, or DRU commander. A copy of such approvals for top secret facilities will be provided to the DCS, G–2 (DAMI–CDS) for review.

f. A completed risk assessment by the responsible commander or civilian equivalent.

g. COMSEC precautions during tactical or combat operations will be established based on existing operational conditions and directives issued by the cognizant ACOM, ASCC, or DRU security officials.

2–24. Protecting passwords

a. Passwords for computers or other devices which contain or protect COMSEC information must be selected and protected in accordance with the guidelines provided by CIO/G–6.

b. Classification of passwords and PINs will normally be assigned the highest classification of any information protected by the password and PIN. If the password and/or PIN is safeguarded so that it cannot be associated with a particular device, the password and PIN may be considered unclassified and/or FOUO.

c. Classified passwords and/or PINs will not be shared or stored in a manner which will allow access or viewing by unauthorized personnel.

2–25. Classified communications security information

Classification principles and procedures, marking, downgrading, and declassification actions directed by AR 380–5 also apply to COMSEC information. The general guidelines for classifying COMSEC information are in appendix B.

2–26. Hand receipting communications security material

The CAM will hand receipt accountable COMSEC material only to authorized persons who have an operational need.

a. Prior to releasing or approving release of COMSEC material, the CAM must verify the recipient's clearance, access restrictions, availability of approved storage and operational facilities, and a need-to-know. The CAM must provide written briefing and instructions to the prospective recipient on how to protect the material. In return, the CAM must obtain a written acknowledgment that the prospective recipient understands and will fulfill all physical protective requirements and employ all mandated security procedures.

b. Accountable COMSEC material will not be hand receipted between COMSEC accounts. Material exchanged between accounts must be transferred. COMSEC material may, however, be hand receipted to individuals, including CAMs.

c. See TB 380–41 for hand receipting procedures.

d. Any requirement for hand receipting to contractors must be included in DD Form 254 and must specifically indicate that the contractor requires access to COMSEC material to perform the mission under the terms of the contract.

e. COMSEC material will not be subhand receipted without written authorization from the CAM. This authorization may be provided on the SF 153 hand receipt or covered in COMSEC SOPs.

f. Procedures must be instituted to verify enrollment in the DACAP at all levels prior to subhand receipting COMSEC material.

g. Unlimited subhand receipting is authorized when there is a requirement to distribute COMSEC material in a combat situation or other potentially hostile environment. A commander is authorized to evaluate the risks related to the physical distribution of cryptographic key and make a determination to subhand receipt COMSEC material within the command multiple levels down. The actual level of authorization will be determined by the commander, documented in memorandum format, incorporated in the local COMSEC SOP, and retained on file in the COMSEC account. Accountability will be maintained at all times.

h. Sub-HRHs will return unused effective or future COMSEC material to the HRH unless they have instructions and authority to destroy the material. Superseded material will be handled under the provisions of TB 380–41.

i. KSV–21 card used with STE may be subhand receipted to the lowest user level.

j. Commanders (and civilian equivalents) responsible for COMSEC accounts will ensure a personnel accounting system is established whereby no HRH may depart the unit without first clearing the COMSEC account of all hand receipts.

k. Inspections will be conducted by the CAM for all HRHs and sub-HRHs as outlined in TB 380–41.

2–27. Protective technology

NSA provides state-of-the-art, tamper-revealing products for information processing equipment and keying material. The level of protection obtainable from these products depends almost entirely upon the inspection and control programs conducted by users. To ensure the integrity of protective technologies, the CAM must ensure that personnel who routinely handle or use protectively packaged keying material or tamper-sealed information processing equipment are trained in the procedures for inspection and disposal of used protective technologies.

2–28. Reproduction of communications security material

Reproduction of classified COMSEC documents will be in the form of extracts. Extracts will be made and controlled as shown below. Except as provided in paragraph *a*, the proponent for the document must approve the reproduction of complete documents.

a. Extracts of COMSEC information are permitted unless specifically prohibited in a document's promulgating instructions. TRADOC training centers and schools, program managers, and USACSLA's New Equipment Training Program have a continuous exception to extract restrictions when extracting COMSEC information to include in lesson plans and examinations. The covers of all lesson materials containing extracts of COMSEC information will cite this paragraph and regulation as authority for the extract.

b. Specific guidance on making extracts of key is contained in either the cryptosystem operating instructions or the key system handling instructions. CONAUTHs have a continuous exception to extract restrictions and may issue portions or complete editions of key, to include printed key in canisters. Issuing segments from a canister is discouraged; however, as it defeats the integrity and protection provided by the canister.

c. Reproduced COMSEC material is not reportable to the central office of record, but is locally accountable until destroyed. See TB 380–41 for accounting procedures.

d. COMSEC material is considered to be reproduced when it has been duplicated in like form (for example, creating a backup copy of a disk) or converted for equipment fill (for example, extracting a key file from a disk and storing it on a key storage device). Converting hard copy key to electronic form for immediate equipment fill is not considered reproduction. Reproduced materiel material must be documented and controlled.

e. Keying material for machine cryptosystems will not be reproduced without the consent of the CONAUTH. If CONAUTH approval cannot be obtained in time to meet operational requirements or if a CONAUTH is not designated the local commander can authorize reproduction. The CONAUTH and the central office of record must be notified at the earliest opportunity.

f. Unencrypted cryptographic algorithms and logic will not be reproduced without the authorization of the NSA Information Assurance Policy, Procedures, and Insecurities Division (I41).

g. Encrypted cryptographic algorithms and logic may be reproduced as necessary. No accounting is necessary for encrypted software. However, sensitive programs, for example, Nuclear Command and Control programs may require additional controls. Such controls will be found in specific systems doctrine, which have precedence over this document. Users must control and track the JOSEKI decrypt key as specified in paragraph 2–12 of this regulation.

2–29. Communications security equipment modification

Unless an operational waiver is in effect, only COMSEC equipment with all approved mandatory modifications applied will be used to secure information systems.

2–30. Destruction of communications security material

Routine destruction of CMCS-accountable COMSEC material.

a. In cases of conflict between this chapter and operational security doctrine for a specific cryptosystem, the operational security doctrine will take precedence.

b. The destruction official and the witness must be cleared for the highest classification of material to be destroyed. Both individuals must be physically present to view the actual destruction. Both are responsible for a properly prepared destruction report that lists all material destroyed and for ensuring that all destruction meets the appropriate standards in TB 380–41. Intentional falsification of COMSEC material destruction reports is subject to administrative and civil sanction, including adverse personnel actions, as well as, criminal sanctions under the Uniform Code of Military Justice (UCMJ) or Federal law, as appropriate.

c. Keying material will be destroyed as soon as possible after it has been superseded, served its intended purpose, or is obsolete.

d. Defective or faulty key will not be destroyed but will be immediately reported to the NSA Information Assurance Directorate (I01P3) and held for disposition instructions.

e. The CAM and alternate CAM will perform monthly or routine destruction of superseded editions of key. However, this routine scheduled destruction will not be used as the basis for delaying immediate destruction of key no longer needed. Destruction of individual key segments or other key media consumed throughout the cryptoperiod will be accomplished immediately in accordance with equipment operating instructions and operational security doctrine. Granting the authority to destroy superseded material to additional appropriately cleared people, who then certify this destruction to the CAM, is preferable to delaying destruction even for a short period of time. The following paragraphs indicate various types of procedures which may be followed in similar situations with emphasis on timely key material destruction in the interest of national security.

(1) In a large facility, cleared operators may be granted authority to destroy keying material they use in the presence of cleared witnesses as soon as the material is superseded. Cleared operators may accomplish destruction by placing the material in an approved destruction device.

(2) In a small facility with only a few pieces of COMSEC equipment, the CAM may personally collect superseded

keying material, replace it with new material, and effect timely destruction of superseded material in the presence of a cleared witness.

(3) In tactical or mobile situations, routine destruction may be accomplished at the using facility by a cleared individual and witness. The user must notify the issuing CAM, either verbally or in writing, that the user has destroyed the material. Verbal notifications must be supported with written confirmation of destruction as soon as possible, but no later than 72 hours after supersession of the edition of key. For accounting purposes, the CAM will then consider the material destroyed. In such cases, the CAM must brief the user of the necessity to promptly and completely destroy superseded keying material and for immediate reporting of any loss of control before destruction could be accomplished.

2–31. Destruction schedule

a. Keying material designated crypto that has been issued for use will be destroyed following expiration of the cryptoperiod, or in accordance with the equipment operating instruction. As a general rule, key material may not be held longer than 12 hours following expiration of the cryptoperiod. However, where special circumstances prevent compliance with the 12–hour standard, local commanders or responsible officials may grant an extension in writing up to 72 hours. In the case of an extended holiday period (more than 72 hours) or when special circumstances prevent compliance with the 12–hour standard (for example, destruction facility or operational space not occupied) destruction may be extended until the next duty day. In such cases, the material must be destroyed as soon as possible after reporting for duty. Used or superseded keying material or extracts carried aboard special purpose aircraft may be retained in secure storage until secure destruction facilities are available, but must be destroyed as soon as possible thereafter.

b. Keying material held in electronic form may continue to be held after loading the key into an end cryptoequipment. The key fill device must have an audit trail capable of indicating when and how many times each key was output from the fill device. The audit trail must either be uploaded (for example, to an LMD and/or KP) where it will be reviewed or viewed on the fill device itself by the local CAM to ensure that only authorized copies of keying material were made and destruction dates match destruction certificates.

c. KEKs must be destroyed as soon as they are filled into the ECU unless specific systems doctrine allows further retention. Other electronic keying material which has been filled into an ECU may continue to be securely stored in an approved key fill device until the end of the key's cryptoperiod, when operationally necessary. The key fill device must create and store an audit trail capable of indicating when and how many times each key was output from the fill device.

Note. The KYK–13 and KYX–15 common fill devices are not authorized to store KEKs after loading into the ECUs. These common fill devices will be zeroized immediately after loading KEKs into the ECUs.

d. Key contained on CIKs (for example, KSD–64) will be eradicated by zeroization as soon as possible after supersession. This will be done using the erase or zeroize functions of the KOK–22A or by following the system operational security doctrine.

e. Encrypted key will be destroyed when no longer needed or upon supersession of the keying material.

f. Destruction of unencrypted key on removable media, unless offloaded to another device or to other approved media, may be accomplished after the last key on the media has been superseded. Operational security doctrine will define destruction requirements for keying material specific to each equipment and key media.

g. Complete editions of superseded keying material designated crypto, which are held by a COMSEC account, will be destroyed within 5 days after supersession.

h. Destruction of encrypted electronic key, which has an associated KEK, may be accomplished by zeroization (or the equivalent) of all copies of the KEK. The zeroization of the KEK should be accomplished as soon as is practical.

Note. Key held on the LMD and/or KP will be destroyed upon supersession of the key.

i. Maintenance and test keying material not designated crypto is not regularly superseded and need only be destroyed when physically unserviceable (or no longer required), unless otherwise directed by specific policy doctrine.

j. Superseded classified COMSEC publications which are held by a COMSEC account will be destroyed within 15 days after supersession.

k. Superseded classified COMSEC aids held at distribution activities (that is, not issued to user COMSEC accounts) will be destroyed within 15 days after supersession; however, more frequent destruction of such material is recommended.

l. The residue of entered amendments to classified COMSEC publications will be destroyed within 5 days after entry of the amendment.

Note. Contingency physical keying material marked crypto that is not enclosed in protective packaging (for example, canisters) with no supersession rate must be superseded and destroyed no later than 6 years after generation or receipt, unless the NSA Information Assurance Policy and Doctrine Division authorizes a longer retention period. The 6–year time limit does not apply to protectively packaged material.

m. Other COMSEC material will be destroyed no later than the 15th day of the month following supersession. Accountable COMSEC publications become superseded upon receipt of new edition.

n. Nonemergency destruction of COMSEC equipment and components is prohibited unless approved and directed, in writing, by the USACSLA National Inventory Control Point Commodity Manager.

o. Protective packaging used with key, such as tape canisters, will be destroyed in conjunction with the destruction of key.

p. The KP keeps track of destroyed electronic key. This is sufficient for electronic key destruction in LMDs at accounts that have a KP.

q. Witnessing is not required for destruction or inventory of electronic key where the destruction or inventory is performed by the LMD and KP.

r. However, witnessing continues to be a requirement for any COMSEC material used in EKMS that must be physically destroyed and inventoried.

s. In high-risk environments, superseded key must always be destroyed immediately. The 72–hour extension authorized in paragraph 2–31*a* does not apply.

2–32. Destruction methods

a. Burning, disintegrating, crosscut shredding, or pulping are the approved methods for the routine destruction of paper COMSEC and classified material. Burning, disintegrating, and chemical alteration are the approved methods for the routine destruction of nonpaper COMSEC and classified material. COMSEC key tape is composed of paper-mylar-paper and will not be destroyed employing methods for COMSEC paper. COMSEC key tapes can only be destroyed by burning, disintegrating, and chemical alteration.

b. The shredder and disintegrator evaluated product lists (available on the secure internet protocol router network at http://www.iad.nsa.smil.mil/resources/library/destruct_guides_section/index.cfm) identify devices that are approved for the destruction of paper COMSEC and classified material. The disintegrator evaluated products lists identify devices that are approved for the destruction of paper COMSEC material and nonpaper COMSEC and classified material.

(1) Floppy disks - degauss, burn, or shred after removing jacket and metal hub.

(2) Hard drives - degauss, smelt to temperature of 2800 degrees Fahrenheit.

(3) Compact disk and digital versatile disk - disintegrate.

2–33. Storage of communications security material

Unless in use by, in the physical possession of, or continuously tended by a properly cleared person or persons where its adequate protection is presumed, CMCS-accountable COMSEC material will be stored per AR 380–5 and TB 380–41.

a. It is Army policy that weapons or sensitive items such as funds, jewels, precious metals, or drugs will not be stored in the same container or facility used to safeguard classified information.

b. The top secret key will always be stored under TPI rules. The top secret key will be stored under TPI controls employing 2 different approved combination locks or a single lock with 2 combinations meeting Federal Specification (FF–L–2740B) with no one person authorized access to both combinations. All persons with access to either of the combinations will have a top secret clearance. Storage can be in a locked strongbox within a security container, in a security container within a vault, or in a security container with 2 combination locks. At least one of the combination locks must be built-in, as in a vault door or in a security container drawer. Neither key locks nor cipher locks will be used to meet the requirement for 2 combination locks. Caution: For facilities in continuous operation (or where unaccompanied individuals are on duty), outer vault doors do not satisfy the 2 barrier protection requirements of TPI. Such facilities require dual combination protection (for example, a dual combination safe) within the facility to store top secret key or the establishment of a no-lone zone.

c. Unencrypted (RED) keying material in electronic form will only be stored in NSA-approved and government-owned key storage devices.

d. The combinations for TPI safes should be protectively packaged separately and held at separate locations. It is understood that there will be situations where a single individual, such as the facility security manager, will have access to protective packages containing both combinations. If the combinations to TPI containers are not protectively packaged, the combinations must be stored at separate locations.

e. Any violation of TPI or no-lone zone control is a reportable COMSEC incident.

f. In those instances where exposed segments of current key must be held in storage for the duration of the cryptoperiod, special emphasis must be placed on their security and accountability.

g. In mobile and transportable conveyances, the current edition and one future edition of key may be stored in a standard GSA-approved field safe or an equivalent container secured by a GSA-approved 3-position combination padlock (FF–P–110J). Mobile and transportable conveyances in which key is stored must have supplemental controls applied that will prevent undetected access to the key or removal of the container in which the key is stored. A guard is required for conveyances or containers that can be surreptitiously removed.

h. In mobile or transportable facilities where in normal storage means are not practical, no more than a single edition of keying material may be stored.

i. COMSEC equipment and components.

(1) When not installed in an operational configuration, unkeyed classified COMSEC equipment must be stored in the manner prescribed in AR 380–5 for material of the same classification.

(2) CCI will be protected under the provisions of this regulation and the Army Standard Logistics regulations.

(3) The commander must approve the storage of keyed COMSEC equipment. When equipment is stored in a keyed condition, storage requirements for the key must be satisfied.

(4) When installed in an operational configuration in either fixed, mobile, or a transportable facility, unkeyed COMSEC equipment may be left unattended, provided the commander has conducted a risk assessment and determined that the risk of unauthorized access is acceptable (see AR 190–51).

(5) Future key, nonoperational and spare COMSEC equipment, and COMSEC publications will not be stored in unattended mobile or transportable facilities.

j. Loading unencrypted keying material (or encrypted keying material with its associated KEK or Transfer KEK (TrKEK) into an electronic fill device is limited to the amount of key authorized by the CONAUTH. CONAUTHs must limit unencrypted keying material to the amount allowed by operational security doctrine.

k. Individual equipment doctrine will specify the amounts of future keying material that may be filled to a specific ECU.

l. Unlimited encrypted keying material may be loaded into an electronic fill device as long as the KEK or TrKEK used to decrypt that key is not present in the same fill device.

m. COMSEC publications such as the cryptographic operational general publication (KAG), cryptographic operational maintenance manuals, cryptographic operational operating manuals and cryptoancillaries (including equipment and software), key not marked crypto, and other cryptographic material not governed by this paragraph will be protected commensurate with its classification per AR 380–5.

n. All COMSEC vaults constructed after June 2000 must meet the standards provided for in appendix C. Those storage facilities certified as vaults prior to the date of this regulation will be considered to meet the requirements of this regulation until such time as they are modified in any way. At that time, they will be required to be brought up to the standards of appendix C or they will no longer be considered vaults for COMSEC purposes.

2–34. Open storage

a. Open storage of classified COMSEC key is prohibited, with the exception of that classified key coded ALC 4. This material will be treated as "other COMSEC material" under paragraph 2–34*b*.

b. Open storage within a COMSEC facility of other COMSEC material classified no higher than secret may be authorized by commanders in writing holding the military rank of lieutenant colonel (O–5) or above (or comparable civilian director), based upon their determination that the risk is acceptable (see chap 3).

c. A vault is a security container in and of itself. Therefore, material stored in a vault is in a security container, regardless of whether it is on a shelf, in a file cabinet, or in a GSA-approved security container.

d. Open storage of an LCMS workstation is authorized based on a commander's local risk assessment, provided the area is an approved secret or higher COMSEC facility. See TB 380–41 for specifics and exceptions.

e. Unencrypted unclassified COMSEC material should be stored in the most secure means available to the user, but at a minimum by a method that will reasonably preclude any chance of theft, sabotage, tampering, viewing, or use by unauthorized personnel.

f. Encrypted software and encrypted keys do not necessarily have special handling or storage requirements but should be treated as unclassified and/or FOUO material. The system or user may require accounting for encrypted software and encrypted key depending on the application.

2–35. Secure cryptographic devices in personal residences

Users must comply with AR 380–5 for storage of collateral information and the by-products of using secure COMSEC equipment. Specific National Security Operations Security Doctrine will take precedence over this regulation.

a. On-post residence. If the device is a CCI, storage will require the use of double barrier protection and separation of CIK or PIN from the instrument when not in use.

b. Off-post residence. Although highly discouraged, the same safeguards for the COMSEC material must be in place. Safeguards must ensure only authorized users have access and any unauthorized access can readily be detected.

2–36. Removable media protection

This paragraph will only address electronic classified National Security Information (NSI) data on storage devices, (for example, hard drives, servers, thumb drives, disks, compact disks, digital versatile disks, or other electronic storage devices. Storage can be either physical protection or the use of NSA Type 1 encryption.

a. Storing noncrypto classified unencrypted Red data must be accomplished in accordance with AR 380–5. Crypto material will be stored in accordance with this regulation and TB 380–41.

b. Classified NSI data must be encrypted by NSA-approved encryption. classified NSI data that has been encrypted by NSA encryption may be stored as unclassified and/or FOUO information. NSI data that has been encrypted onto a removable media by NSA encryptions must still be controlled as secret classified media due to computer security rules that state when media is entered in a classified system the media assumes the classification of the system.

2–37. Transferring communications security material

a. Transfers of COMSEC material will be documented in accordance with the policies and procedures contained in this regulation, TB 380–41, and instructions of the central office of record. CAMs that transfer material must ensure they receive a signed receipt digitally or wet signature. Unencrypted key will not be transferred between COMSEC accounts without CONAUTH approval.

b. COMSEC software (collateral COMSEC material) which has been encrypted is not accountable in the CMCS. As long as it remains separate from its decrypt keying material, it may be handled as unclassified and/or FOUO data that requires no audit or accounting.

c. Unencrypted non-COMSEC software (for example, mission data or radio parameters) may be handled as nonaccountable data. If the software is classified, it must be protected at the appropriate classification level.

d. Encrypted keying material is normally unclassified and/or FOUO and not crypto. However, packages which contain encrypted keying material (not the keying material itself) may be initially marked as unclassified crypto for ease of distribution and control. A package containing encrypted keying material received by a CAM must be accounted for as CMCS accountable material until it is issued to a user. Once issued to a user and signed for no further accounting by the CAM is necessary.

e. Unencrypted keys will remain crypto. Keys that are decrypted and exposed to human view or intervention must be accounted for in the CMCS. Keys decrypted in machine systems which are not human accessible need no additional accounting.

2–38. Transportation of communications security material

The possibility of compromise is increased during shipment. All persons who handle COMSEC material must be carefully instructed in handling procedures. This includes proper methods of emergency destruction to prevent compromise during transportation. The requirements in this paragraph, AR 380–5, TB 380–41, and Army Standard Logistics regulations apply to the transportation of all COMSEC material.

a. COMSEC material shipments under contingency deployment and under courier escort by U.S. military personnel must be exempt from customs inspections by any U.S. or foreign customs officials. Arrangements will be made to conduct pre-deployment inspection or screening of COMSEC material at a secure location at the home station prior to sealing containers. Once inspected, banded, sealed, and properly labeled, (certifying inspection by customs officials), the containers must not be opened until arrival at the deployment site by the CAM.

b. Key will be transported as follows:

(1) For top secret key, TPI will be applied whenever unit couriers transport top secret key between COMSEC accounts or HRHs and local elements. Two persons who are cleared for top secret and authorized to receive the material must sign receipts for this material. The key must be double-wrapped while in transit in accordance with AR 380–5. TPI controls are not required for top secret key while it is in the custody of the defense courier service or the U.S. Diplomatic Courier Service.

(2) The secret key must be transported by the defense courier service, an officially designated unit courier, or U.S. Diplomatic Courier Service. Secret key or higher may not be sent by registered mail without the specific prior approval of DCS, G–2 (DAMI–CDS).

(3) For confidential and unclassified key, U.S. registered mail may be used to transport key to recipients served by U.S. Postal Service (USPS) facilities. However, the mail must not pass out of the control of the USPS and must not pass through a foreign postal system or any foreign inspections.

(4) Any U.S. flagged commercial airline can be used to carry key within the U.S.. Outside the U.S. the use of non-U.S. flag aircraft or any foreign-owned, controlled, or chartered carrier to carry key is strongly discouraged because of the threat by terrorists and lack of U.S. control. The ACOM, ASCC, or DRU commanders may, in cases of operational necessity, approve the use of such carriers when limited quantities of future key must be carried. Quantities will be limited to no more than four editions of quarterly or more frequently superseded material or 2 editions of semiannually or less frequently superseded material. Sufficient time should be available before implementation (at least 3 days) to supersede the material should it be compromised. The ACOM, ASCC, or DRU commanders may delegate this authority to the lowest general officer level.

(5) Key will be packaged separately from its associated COMSEC equipment unless the application or design of the equipment is such that the key cannot be physically separated.

(6) Key in any form must be transmitted electronically whenever possible using approved methods as outlined in National Advisory Group (NAG)–16 or NAG–53, or via EKMS. However, when transmitting physical key that has been converted to electronic form or electronic generated key, the user(s) must ensure the communications systems

used are capable of providing end-to-end security that is equal to or higher than the classification of the transmitted key. The key setting must not appear in the plain text anywhere in the communications path.

c. COMSEC equipment will not be shipped or transported in a keyed condition. This restriction does not apply to tactical movements or in emergency situations where equipment must remain keyed for critical mission accomplishment. Electronic fill devices may be transported in a loaded condition by authorized individuals, provided adequate security measures are employed by the couriers and the equipment CIKs are removed and carried separately.

d. COMSEC equipment will be transported as follows:

(1) Shipments of COMSEC equipment classified secret will be transported by the Defense Courier Service, U.S. Diplomatic Courier Service, officially designated unit courier, or an authorized cleared commercial carrier using protective security services (applies only when shipping within the U.S. and its possessions and territories, where the equipment will not leave U.S. control and be subject to foreign intervention, customs, or inspections).

(2) All key production equipment, including the EKMS Key Processor (KOK–22), must be transported by Defense Courier Service or authorized courier.

(3) Shipments of COMSEC equipment classified confidential may be transported by any means specified in paragraph 2–38*d*(1) or by—

(a) U.S. registered mail provided it stays within U.S. control at all times and does not pass through a foreign postal system or any foreign inspection.

(b) U.S. military or military-contractor air service (for example, Air Mobility Command and Logistics Aircraft) provided that a continuous chain of accountability and custody for the material is maintained while in transit.

(4) Unclassified COMSEC equipment designated CCI will be transported under the provisions of chapter 8 of this regulation.

(a) Unclassified COMSEC equipment not designated CCI may be transported by any means approved for the transport of high-value Government property.

(b) Domestic commercial passenger trains, airlines, and buses may be used by couriers at the discretion of the appointing commander, provided the provisions of AR 380–5 are followed.

(c) Within the continental United States, when operational necessity dictates, confidential and secret COMSEC equipment (zeroized) installed in standard military equipment shelters may be transported via uncleared commercial carriers, provided all of the provisions of TB 380–41 are met.

e. Cryptographic media which embody, describe, or implement a classified cryptographic logic, such as full maintenance manuals, cryptographic logic descriptions, drawings or cryptographic logic, or specifications describing a cryptographic logic and cryptographic computer software will be transported by cleared couriers, the Defense Courier Service, or U.S. Diplomatic Courier Service. These media may not be sent through any postal system.

f. Other classified COMSEC material that does not embody, describe, implement, or contain a classified cryptologic may be transported in the same manner as the material described in paragraphs *a* and *b*, and if classified secret or confidential, by a cleared commercial carrier under DOD 4500.9–R or by USPS registered mail. The provisions of AR 380–5, relative to the use of commercial passenger aircraft, also apply to these shipments.

g. When operationally required, COMSEC equipment and COMSEC material may be airdropped, unless prohibited by a specific equipment publication, provided the material is under the control of a properly cleared person until the material leaves the aircraft and the commander has determined that there is a high probability of immediate recovery by authorized persons.

h. Vehicles or equipment shelters in which COMSEC equipment is installed may be transported by helicopter using sling-load techniques. Equipment should not be keyed unless there is an operational requirement for its immediate use upon landing. Associated key will not be sling-loaded, but may be carried inside the helicopter moving the vehicle or shelter.

i. COMSEC material required in support of forward area tactical operations may be air transported across hostile territory.

j. Upon receipt, all packages containing classified COMSEC material will be inspected for evidence of penetration. If evidence of tampering is found, a COMSEC incident report will be submitted under the provisions of chapter 6. Packages and containers will be opened by the authorized addressee only within 2 working days after receipt. The addressee will report any discrepancies to the central office of record and to the shipper as specified in this regulation, TB 380–41, or AR 735–11–2, as appropriate. However, unit packs in original manufacturer or depot sealed packages will not be opened except when there are signs of tampering, the material is to be used, or a physical security check is required. For inventory purposes, use the external packaging label.

k. Packaging of classified COMSEC equipment will be done under the provisions of AR 380–5. Packaging of unkeyed CCI will be in accordance with this regulation and Army Standard Logistics regulations.

l. Couriers for COMSEC material must be specifically designated in writing (DD Form 2501, Courier Authorization Card is recommended) by an authorized official within the individual's chain of command. In addition, official signed courier orders with detailed instructions and identification of material being hand carried must be provided to the courier.

m. It is the responsibility of the CAM directing movement of the material to ensure that all couriers are properly

cleared, trustworthy, and briefed on their responsibilities for safeguarding the material entrusted to them. Couriers must be provided instructions covering emergency situations including loss or other compromise of the material in their possession.

n. Couriers traveling outside the continental U.S. will have their request for courier orders forwarded through the unit or activity security manager for approval. Couriers must be provided the telephone number of the nearest U.S. embassy or consulate in every country through which they will travel. The identification card and letter of authorization requirements contained in Federal Aviation Administration Advisory Circular 108–3 available at http://rgl.faa.gov/Regulatory_and_Guidance_Library/rgAdvisoryCircular.nsf/list/AC%20108-3/$FILE/AC108-3.pdf) must be complied with.

o. Transportation of cryptographic algorithms or logic. Unencrypted cryptographic algorithms and logic will not be transported without the approval of the NSA program manager for the associated equipment. All unencrypted or unprotected (by antitamper coating) cryptographic algorithms or logic must be transported by one of the following methods:

(1) Defense Courier Service.

(2) State Department Courier Service.

(3) Formally designated and appropriately cleared couriers.

p. Encrypted cryptographic algorithms and logic may be sent by any available means as long as their associated decryption key is sent by approved means in a different shipment.

q. Both key and other data (for example, encrypted algorithms and software) may be moved between approved user organizations via the KMI as capabilities allow.

Chapter 3
Communications Security Facilities

3–1. General

The term COMSEC facility is defined in the glossary. Depending upon the functions being performed, a COMSEC facility may consist of one or more GSA-approved steel security container(s) located in a room or office (in the case of multiple security containers, they must be collocated within the room or office). Or it may consist of a room, a suite of rooms, a vault, or an entire building. Security requirements for COMSEC facilities will be established based upon the functions being performed, the classification of the material involved, and the information being handled.

a. A USACSLA-approved COMSEC facility is not required to store, house, or operate CCI equipment. However, a local risk assessment and command approval is required.

b. USACSLA-approved COMSEC facilities are exempt from the physical security inspections under AR 190–13. Refer to TB 380–41 for specific procedures and guidelines for establishing and maintaining a COMSEC facility. Such facilities will normally be designated as restricted areas per AR 190–13 (see para *c*).

c. In those instances where, due to operational necessity a larger facility is not required, a COMSEC facility may consist of nothing more than a GSA-approved security container or multiple containers in a common administrative office area, provided adequate safeguards are present to inhibit unsupervised or surreptitious access to the GSA-approved containers by unauthorized individuals. At the discretion of commanders, when the GSA-approved security container constitutes the entire COMSEC facility, designation of that facility or area in which it is located as a restricted area may be waived.

d. For those facilities operated by CAMs administering a service authority approved COMSEC account, CFA will only be granted by USACSLA per this regulation and TB 380–41.

3–2. Communications security facility approval

a. USACSLA approval of a COMSEC facility to operate a COMSEC account is required before a CAM may request COMSEC material and will be granted under the authority of this regulation. Procedures for establishing a COMSEC facility are contained in TB 380–41.

b. Approval is based on an evaluation of information given in the COMSEC facility approval request (CFAR). The CFAR will state the physical protective measures and security procedures in place, to include specific TPI protection for top secret accounts. It will also state whether the account is or will be an automated LCMS workstation account or manual accounting system using item register cards. The CFAR will also contain a statement that the commander has evaluated the risks to the facility and found them to be acceptable.

c. The need for a COMSEC facility for a HRH will be determined by the CAM based on unique circumstances, such as large volume of required material, the type of material, and operational environment. The basis for this approval will be the same as that in paragraph 3–2*b*. These COMSEC facilities do not require USACSLA approval, but must adhere to the procedures outlined in TB 380–41. The CAM is responsible for inspecting HRHs facilities and

maintaining a record of all HRH COMSEC facilities for which their account is responsible. The CAM is also responsible for ensuring those applicable provisions of this regulation and TB 380–41 are complied with by the HRH.

3–3. Communications security facility approval request

All CFARs submitted to USACSLA for approval will be in memorandum format (see TB 380–41), with a completed (minus the account number that will be assigned by USACSLA) CARP attached, signed by the commander, civilian equivalent, or senior staff officer granted delegation of authority and submitted through established Army command channels to USACSLA for approval. All CFARs and CARPs for contractor accounts will have a DD Form 254 attached. Once the facility is approved, USACSLA will establish the COMSEC account and provide the unit an account number.

3–4. Duration of communications security facility approval

A COMSEC facility approval remains valid as long as the physical protective measures and security procedures that were the basis for the approval remain substantially unchanged. When a COMSEC facility approval is invalidated, USACSLA will stop shipment of material until the COMSEC facility approval is reinstated. When the Director, USACSLA, declares that protection is inadequate, USACSLA will direct the return of all CMCS accountable material.

a. In those instances where the COMSEC account is contained completely in an approved GSA security container, a new approval is not required when relocating the container within the same building if the physical security standards do not change. However, a memorandum change to the CARP reporting the new location of the container must be submitted to USACSLA (SELCL–SAS), Fort Huachuca, AZ 85613–7090.

b. When a COMSEC account has shown no activity for 12 months, USACSLA will advise the unit commander through command channels that the COMSEC account is targeted for closure because of inactivity. The unit commander will be allowed 60 days to justify a continuing requirement for the account. If none is provided, USACSLA will issue disposition instructions for all CMCS accountable material and close the account.

3–5. Safeguarding communications security facilities

This paragraph prescribes the physical protective measures and security procedures for COMSEC facilities.

a. COMSEC facilities will be located in areas that provide positive control over access. When possible, they should be away from areas such as parking lots, ground-floor exterior walls, multiple corridors and driveways, buildings, or office space in which it is difficult or impossible to affect access control or high-risk environments.

b. COMSEC facilities established in permanent structures will be provided the required protection equivalent to the level of classification of the COMSEC material held in that facility. The physical security standards available in appendix C of this regulation and TB 380–41 will be used as guidance to establish specific construction criteria for new facilities designed to house COMSEC accounts that are large enough to require a separate facility or vault.

c. When a COMSEC facility consists of a security container or series of security containers, they must be located in an area that provides sufficient additional protection to prevent undetected, unauthorized removal of the security containers. This may be accomplished as simply as placing the containers in a room with a key lock and controlling access to the keys.

d. Access to a COMSEC facility will be granted based on a person's duties, need-to-know, and security clearance. A current approved access list will be maintained in each COMSEC facility. Personnel not on the access list will be escorted at all times while they are in the facility by a responsible person whose name appears on the access list. All persons who require an escort must sign the DA Form 1999 (Restricted Area Visitor Register) prior to entering the facility.

e. When the facility is one or more GSA-approved security containers, DA Form 1999 to register visitors is not required. Access to the container will be restricted to those individuals identified on SF 700 (Security Container Information).

f. Guards who have access to classified COMSEC material must meet the access requirements of paragraph 2–8. Area control guards who cannot gain access to COMSEC material do not need to meet the requirements for access. Guards who are not U.S. citizens will only be used where it is not possible for them to gain undetected access.

g. Locks on storage cabinets, safes, vaults, and secure rooms. All COMSEC facilities must comply with AR 380–5. Army units and facilities (including ARNG and U.S. Army Reserve) and Army contractors operating or storing COMSEC material, regardless of the classification of the information or material, will replace existing mechanical combination locks with locks conforming to federal specification FF–L–2740B (XO–7/XO–8/XO–9) electro-mechanical combination locks using the lock replacement prioritized categories and guidance specified in that regulation.

h. During command inspections and USACSLA audit and inspections, any account that has not met the requirement of paragraph 3–5*g* will receive an automatic unsatisfactory rating. In addition, this must be reported as a physical COMSEC incident in accordance with AR 380–40 and TB 380–41. New COMSEC facility approvals will not be granted unless units have complied with AR 380–5 guidance for installing electromechanical combination locks.

i. Lock combinations to COMSEC facilities, including cipher locks used to control access, will be changed—

(1) When placed in use.

(2) Whenever an individual knowing the combination no longer requires access.

(3) When the combination has been subjected to possible compromise.

(4) When the lock is taken out of service.

(5) When any repair work has been performed on the lock.

(6) At least annually.

j. The following personally owned equipment may be introduced into a COMSEC facility with the approval of the CAM:

(1) Electronic calculators, spell checkers, wrist watches, and data diaries. If equipped with data ports, the CAM will ensure that procedures are established to prevent unauthorized connection to automated information systems.

(2) Receive only pagers and beepers.

(3) Audio and video equipment with only a playback feature (no recording capability) or with the record feature disabled or removed.

(4) Radios (receive only).

k. The following personally owned electronic equipment is prohibited in COMSEC facilities:

(1) Photographic, video, and audio recording equipment.

(2) These include, but are not limited to: personal digital assistants, handheld and laptop computers, workstations and associated media, cellular telephones, Web-based phones, 2-way pagers, wireless email devices, and portable music players or devices with memory.

(3) Microphones.

l. Nothing in this regulation will be construed to contradict or inhibit compliance with the law, such as the Americans with Disabilities Act, building codes or federal antiterrorism standards or other applicable statues.

m. The following U.S. Government-owned or U.S. Government-leased equipment are prohibited in COMSEC facilities unless approved by the CAM for the conduct of official duties:

(1) Two-way transmitters (including cellular telephones).

(2) Recording equipment (audio, video, and optical).

(3) Test, measurement, and diagnostic equipment.

n. NSA Certified Cryptographic Equipment (including the SME-personal electronic devices, Sectera GSM phones, and SECNET–54 wireless devices), may be introduced into a COMSEC facility if used in accordance with the applicable operational security doctrine and approved by the CAM.

3–6. Army communications security supplement to DOD industrial security regulations and manuals

a. This paragraph implements, within DA, national policy concerning the release of COMSEC material to U.S. commercial contractors and the establishment and administration of Army COMSEC accounts at contractor facilities. A copy of this regulation may be provided to contractors when necessary to prepare a request for proposal or to meet the requirements of DD Form 254.

b. Applicable provisions are contained in DOD 5220.22–M, DOD 5220.22–R, and AR 380–49.

c. In view of the objectives of DOD 5220.22–R, to ensure its uniform and effective application throughout industry, the content of this section is limited to the minimum supplementation consistent with Army operations. In addition to the policy and procedures contained in the documents listed above, the instructions in paragraph *d* apply.

d. Contractor-installed, contractor-maintained, and contractor-operated COMSEC equipment are handled as follows:

(1) Maintenance personnel assigned to maintain COMSEC equipment in fulfillment of an Army contract will be certified as meeting formal training requirements mandated in AR 25–12. A DD Form 1435 (COMSEC Maintenance Training and Experience Record), will be maintained on all maintenance personnel and validated annually.

(2) Contractor personnel must have received Security Awareness Training and a completed DD Form 2625 (Controlled Cryptographic Item (CCI) Briefing).

(3) COMSEC equipment in operational use must have all NSA-mandated modifications applied.

e. Access to classified COMSEC information may be granted to all contractor employees who are U.S. citizens, who have been granted a final security clearance by the U.S. Government and have a need-to-know. Confidential clearances are not valid for access to classified COMSEC information. In addition to the above, the Army must formally authorize a contractor employee access to classified COMSEC information or a key as stipulated on DD Form 254 made part of the contract. The same applies to those who install, maintain, or operate COMSEC equipment for the Army. A statement that contractor personnel are subject to the DACAP should be included in the DD Form 254, remarks section. The provisions of chapter 2 also apply.

3–7. Continuity of operations plans

a. A COOP and SOPs are required by all COMSEC accounts.

b. The contents of a COOP and SOPs must be tailored to the organization, its mission, operational environment, and based on a risk assessment, conducted by the responsible commander in accordance with AR 190–51.

c. A COOP and SOPs are subject to inspection and evaluation by command inspectors, but are not subject to review by USACSLA auditors.

d. TEMPEST considerations – The KP meets requirements of KAG–30A/TSEC and NSTISSAM TEMPEST/1–92. When developing or revising a COOP and similar plans for emergency relocation of a COMSEC account, user organizations must consult CNSSI No. 7000 to determine applicable countermeasures for the LMD and for the facility in which it is placed. A certified TEMPEST technical authority must conduct or validate all TEMPEST countermeasure reviews.

Chapter 4
Controlling Authority Duties and Cryptosystems Management

This chapter establishes the responsibilities of Army CONAUTHs for electronic and physical keying material. CONAUTHs have certain responsibilities and prerogatives relating to the material they control. This chapter establishes those responsibilities and provides guidelines for compromise recovery.

4–1. Controlling authorities

With the advent of EKMS, electronic key generation can occur at all levels within the CMCS, from Tier 0 (NSA), Tier 1 (central office of record), and Tier 2 (operational COMSEC accounts). Commanders at the user (Tier 2) level must recognize and understand that when they direct the CAM to generate local key via their LCMS workstation to establish and provide cryptographic key support to operational networks, the command and its operational staff become the CONAUTH for that key and assume responsibility of this regulation to provide all CONAUTH services to net members using the key. The commander may delegate CONAUTH responsibilities to a trusted subordinate technically qualified to perform these duties, but the ultimate responsibility for fulfillment of all CONAUTH responsibilities with regard to the protection and use of that key rests with the operational commander.

4–2. Controlling authority appointment

a. When a new cryptonet is established, a CONAUTH will be appointed by the commander directing the establishment of the cryptonet to manage the operational use of keying material assigned to the cryptonet. The CONAUTH should be organizationally senior to cryptonet members. The CONAUTH must have the expertise to perform essential management functions and must have the authority to ensure its instructions are carried out. All net members, including members from other departments or agencies, must adhere to the direction given to the cryptonet by the CONAUTH.

b. Since a cryptonet supports an operational requirement, the operational organization directly supported by, or most closely associated with, the cryptonet will normally be assigned CONAUTH responsibilities. CAMs will advise CONAUTHs regarding proper COMSEC logistics support procedures.

c. For locally generated key in electronic form, the commander or civilian equivalent that directs the key generation will perform the CONAUTH functions unless those functions are specifically assigned to another organization.

d. Commanders at all levels may direct a change in CONAUTH appointment under their command. When such change occurs, all cryptonet members, affected distribution activities, and NSA must be notified immediately.

4–3. Controlling authority responsibilities

CONAUTHs direct the establishment and operation of the cryptonet and manage the operational use of material assigned to the cryptonet. CONAUTHs duties apply to the use of both electronic key accountability and physical key. The CONAUTH is the individual directly responsible to the commander for the establishment and operation of the cryptonet (for example, network manager). The CONAUTH is responsible for the following:

a. Identifying and validating cryptonet requirements.

b. Establishing the cryptonet.

c. Evaluating COMSEC incidents and insecurities.

d. Initiating recovery and reconstitution actions.

e. Authorizing key replacement and resupply.

f. Directing classification changes for key (see para *v*).

g. Establishing cryptoperiods and approving extensions.

h. Specifying implementation and supersession dates for key.

i. Specifying key change times.

j. Determining unused key status.

k. Approving the issuance of extracts of key (for example, segments from a canister) and the local reproduction of physical key.

l. Performing cryptonet evaluations at least annually.

m. During contingency operations, temporarily delegate operational net control of appropriate systems to a regional command or net control center in the forward contingency area.

n. CONAUTHs must understand the operational requirements supported by the cryptonet and must be familiar with the operation, capabilities, and doctrinal requirements of the associated equipment or offline system.

o. For cryptonets using hard copy keying material, CONAUTHs will coordinate the establishment and logistic support of the cryptonet by advising appropriate distribution authorities and NSA of the COMSEC accounts that are to receive keying material and the number of copies they will receive.

p. CONAUTHs for off-line cryptosystems must identify specific operational requirements to NSA.

q. CONAUTHs for keying material must specify the initial implementation and supersession dates and inform all cryptonet members, appropriate distribution authorities, and NSA.

r. Supersession rates (the rates at which the editions are replaced) are established by NSA based on physical and cryptographic security considerations, operational need, production, and resupply constraints. Except in emergencies, CONAUTHs will not change supersession rates without proper coordination; for example, a CONAUTH will not arbitrarily convert an annually superseded key to a monthly superseded key. However, a CONAUTH may extend the effective dates of an edition to make use of spare settings when resupply is uncertain.

s. In situations where material cannot be supplied in time to meet operational requirements, CONAUTHs can authorize replacement or resupply of key for machine cryptosystems. KEK must be physically distributed in all but emergency situations, where the alternative is unencrypted communications. The routine distribution of KEK via over-the-air rekeying is prohibited.

t. Manual cryptosystems (codes, authenticators, and call signs) can be locally reproduced as necessary to meet operational requirements. CONAUTH approval is not required, but material must be issued only to users approved by the CONAUTH. Reproduced material must be accounted for in accordance TB 380–41.

u. If hard copy keying materiel or off-line cryptosystems are being used, CONAUTHs must notify all net members, appropriate distribution authorities, and NSA of any changes in cryptonet structure or keying material status. This includes any changes in keying material effective or supersession dates.

v. CONAUTHs will approve classification changes for the key they control. Before upgrading keying material to top secret, CONAUTHs must ensure that it was held under TPI, or that at a minimum, access was restricted to COMSEC account personnel. CONAUTHs must inform NSA of any classification changes.

w. CONAUTHs must maintain accurate records on pertinent aspects of the cryptonet in sufficient detail to manage the membership of the cryptonet and assess the impact of and to recover from a compromise. CONAUTH records must show the identity and validate the membership of all cryptonet members, the amount of material each is authorized to hold, the distribution authorities that support the cryptonet, and the most expeditious ways of promulgating supersession and other emergency information to all cryptonet members.

x. CONAUTHs will contact cryptonet members at least annually. At a minimum, CONAUTHs will identify the material they control and advise net members how to contact them under normal and emergency circumstances. CONAUTHs are authorized to communicate directly with cryptonet members.

4–4. Communications security planning

The Army goal is encryption of all electrically transmitted information through generation and distribution of electronic key. Until total encryption can be achieved, COMSEC planning will include the following:

a. Optimum use of available telecommunications systems employing online COMSEC equipment for protecting all electrically transmitted information.

b. Use of manual and auto-manual COMSEC systems in those situations where online COMSEC equipment is unavailable or not suited for the mission.

c. Although not a COMSEC system, the use of protected distribution systems should be considered in those situations where online COMSEC equipment and manual or auto-manual systems are not available or are unsuited for the mission.

4–5. Emergency requirements for Communications Security Materiel Control System key support

The CLSF will satisfy emergency requirements for physical key distributed through the CMCS from reserve stock. CONAUTHs will request emergency resupply from their CLSF. The CLSF will notify USACSLA and NSA of the resupply action.

4–6. Stockage levels for key

a. Normally, no more than 4 editions of a physical key distributed through the CMCS will be held in user accounts. Resupply actions and unforeseen changes in usage may necessitate exceeding this level. However, a supply of 6 editions (to include the current effective edition) will not be exceeded without prior approval from DCS, G–2, (DAMI–CDS).

b. Six editions of an irregularly superseded physical key distributed through the CMCS may be held even though the usage rate for such material is less than one edition per month. When the usage rate is more than one edition per month, the CONAUTH will establish stockage levels for a 6-month period.

4–7. Requests to establish cryptonets (requests for key)

a. All requests to establish cryptonets using CMCS distributed key, except Secure Data Network System and STE, will be validated by the next higher headquarters or ACOM, ASCC, or DRU before being sent to USACSLA to be filled.

b. USACSLA can provide assistance in determining key requirements, the most suitable cryptosystem, and the best possible cryptonetting scheme.

c. The Army will use electronic key generation and distribution through the EKMS as its primary source. Establishing cryptonets using physical key is an exception and will require specific justification.

(1) Units may request dual media key if total EKMS functionality does not exist.

(2) On the annual Cryptonet Evaluation Report, the CONAUTH will be required to justify any continued use of physical key.

(3) Once a cryptonet is capable of using electronic key, USACSLA will discontinue directing the shipment of the physical key unless the CONAUTH can justify a continued need.

(4) Any new cryptonets established after the implementation of an LMD and/or KP workstation will automatically be issued electronic key unless they have justification to retain physical key.

4–8. Issue of key

a. The CONAUTH will establish the amount of key that may be issued to users. Only that amount necessary to satisfy the immediate operational requirement, consistent with local resupply capabilities, should be issued.

b. Issue of physical key to users may be in whole editions, an extract of an edition, or a key tape segment. The issue of segments from a key canister is discouraged as it defeats the tamper protection provided by the canister. The issue of electronic key in segments is a common accepted practice.

c. Editions or extracts (segments) of editions carried on special purpose aircraft (such as, airborne command posts) will be limited to the amount needed for the mission.

4–9. Use of a classified key

In cases of operational necessity, key may be used to encrypt information classified one level higher than the classification of the key. For example, confidential key may be used to encrypt secret information. Operational necessity will not be construed to apply to situations of a continuing nature. In emergency situations, key that provides the greatest security protection available should be used to protect classified information, regardless of its classification. Key that is not classified will not be used to pass classified information. Classified key will not be downgraded or declassified without specific written authorization from the CONAUTH.

4–10. Cryptoperiod extensions

A cryptoperiod is the length of time each key setting is authorized for use. Cryptoperiod should not be confused with effective period, which is the length of time an edition is authorized for use. Extending the effective period of an edition to make use of spare key settings is not considered extending the cryptoperiod, but is the prerogative of the CONAUTH. CONAUTHs who extend cryptoperiods for reasons other than logistics necessity should follow the guidelines contained in this chapter.

a. When operational requirements necessitate, CONAUTHs can extend the cryptoperiod, unless the specific cryptosystem doctrine prohibits cryptoperiod extensions. In cases of conflict, cryptosystem doctrine takes precedence. This authorization applies to both hard copy and generated key in electronic form. CONAUTHs are not required to report these extensions to NSA. Net members can extend cryptoperiods up to 2 hours to complete a transmission or conversation in progress at key change time. CONAUTH approval is not required and net members are not required to report these extensions.

b. When user accounts have only 2 editions of future key remaining, the CONAUTH must promptly ascertain the status of follow-on material. If net members cannot be ensured of resupply before their remaining key is expended, the CONAUTH must extend the cryptoperiod in accordance with paragraph 4–11. If the extension is insufficient or a resupply date cannot be determined, CONAUTHs must report at immediate precedence to NSA, who will provide additional instructions. The message must include the short title, number of net members, and explain the necessity for the cryptoperiod extension.

Note. When time is of the essence, CONAUTHs can verbally request cryptoperiod extensions from NSA on (301) 688–6860, defense switched network (DSN) 235–6860. Outside of normal duty hours, CONAUTHs should call the NSA senior information systems security coordinator on (301) 688–7003, DSN 235–7003. When authorization is given verbally, CONAUTHs must take immediate action and not wait for message documentation. Net members must abide by all verbal instructions relayed by the CONAUTH.

4–11. Guidelines for extending cryptoperiods

a. When cryptoperiods must be extended for reasons other than logistics necessity (for example, under prestrike, battlefield, or field training conditions), CONAUTHs are strongly encouraged to conduct a risk assessment prior to

implementing the extension. CONAUTHs should consider the following factors before making a decision as to the length of time a cryptoperiod will be extended.

(1) *Size of the cryptonet.* Key used on a large cryptonet is usually more vulnerable to compromise than key used on a small cryptonet because it is available at more locations and more people have access to it. Also, large nets generally carry higher volumes of traffic than small nets. The compromise of a key used to secure a large net could make considerably more intelligence available to an adversary. It is for these reasons that CONAUTH should keep their cryptonets as small as operationally feasible.

(2) *Location and operating environment of net members.* Net members located in the U.S. and its territories and its protectorates are usually considered to be at less risk than those in other locations. Net members located in a high risk environment (for example, in an area outside the U.S. where there is a small or no U.S. or allied military presence or where the political climate is unstable) have an increased risk of physical compromise. Mobile and tactical users have a greater opportunity for loss (particularly undetected loss) of material than do fixed plant net members. In addition, loss on the battlefield could pose an immediate threat not only to U.S. communications but also to U.S, Coalition, or Allied Forces.

(3) *Sensitivity and perishability of traffic.* The CONAUTH should consider the classification of the information being protected, but also whether the information is of long-term or short-term intelligence value. Compromise of a key used to secure upper echelon strategic communications would have a more devastating effect on U.S. security than would the compromise of a key used to secure highly perishable or lower echelon tactical communications. It is for this reason that a single short title "top to bottom" key distribution should be avoided whenever possible.

(4) *Emergency Supersession Plan.* The CONAUTH should have a plan for replacing compromised key. They should know approximately how quickly the key can be replaced and if the plan is realistic in a worst case scenario. CONAUTHs are highly recommended to test the plan annually, because it is extremely difficult to accomplish an unscheduled rekey in a large net without creating additional problems and confusion. It is essential that the CONAUTH know the logistics channels that support the cryptonet, as well as, the electronic key transfer or distribution capabilities of the associated equipment.

(5) *Operational impact of an extended cryptoperiod.* The CONAUTH should make an honest assessment as to whether a cryptoperiod is being extended out of operational necessity or for operator convenience. Although loss of (or the risk of losing) critical communications under battlefield conditions is intolerable, peacetime training is to prepare Army Forces for wartime.

b. If cryptoperiod extensions are necessary to maintain critical communications during battle (actual or training), the following guidelines should be followed:

(1) All preplanned cryptoperiod extensions should begin with a new key setting.

(2) Whenever possible, cryptoperiods should be extended by net and not by short title.

(3) All affected nets should be directed to rekey as soon as there is a break in activity.

4–12. Communications security incidents

a. The CONAUTH must ensure that when the keying material is used by members of more than 1 department or agency, cryptonet members know how to address COMSEC incident reports.

b. CONAUTH responsibilities regarding COMSEC incidents are limited to initiating precautionary supersession or other recovery actions when warranted and rendering an evaluation as part of the administrative closure. Related items such as recommending procedural changes or disciplinary action are outside of the CONAUTH’s purview, except when the CONAUTH is also in the responsible individual’s chain of command.

4–13. Incident evaluation

CONAUTH will evaluate physical COMSEC incidents as specified in chapter 6 of this regulation and TB 380–41. CONAUTH must inform the Army COMSEC Incident Monitoring Activity and NSA of all evaluations.

4–14. Compromise recovery

Compromise recovery and incident evaluation are 2 separate distinct actions that are required of a CONAUTH. Where substantial evidence exists that COMSEC material has been compromised, the CONAUTH must take immediate action. The CONAUTH will not wait for incident reporting and evaluating requirements to be satisfied, but will initiate recovery action as soon as they have enough information to make an informed decision. The CONAUTH will announce precautionary supersession of electronic key immediately when a compromise cannot be ruled out, unless operational conditions preclude such action. See paragraph *b*.

a. The feasibility of superseding hard copy keying material is contingent on several factors: the number of editions held at the user level, the capability of NSA to produce keying material, and the distribution authority’s capability to supply replacement editions. Any decision to supersede must take into consideration the time required to notify all cryptonet members and implement the new material. Emergency supersession of hard copy key must be reported immediately to appropriate distribution authorities and NSA so that resupply action may be taken, replacement material may be produced, and status documents corrected.

b. Superseding electronic key can present a unique problem for mobile or tactical users. Some of the communications paths used to deliver the key may no longer exist due to the redeployment of some of the relaying units. The CONAUTH must consider the time needed to create or reestablish communications paths before directing supersession.

c. The following options are available to the CONAUTH when supersession is warranted, but not all net members hold replacement key. In order of preference:

(1) Except as noted in paragraph 4–3*s*, key may be electronically generated and transmitted to net members via an uncompromised cryptosystem approved for over-the-air key transfer.

(2) Printed key settings may be transmitted by a cryptosystem that provides end-to-end encryption equal to the classification of the transmitted key (for example, Defense Management System and Automated Message Handling System message distribution systems, secure facsimile, or secure telephone). Printed key settings can also be encrypted by auto-manual or one-time pad system and transmitted over a system that is secured at a lower level than the encrypted key.

(3) Printed key settings may be reproduced and physically transferred to net members. Punched tape will not be reproduced without the authorization of NSA. Converting hard copy keying material to electronic form for equipment fill is not considered reproduction.

(4) Key may be physically transferred to net members in a common fill device or other approved transfer device. When keyed, the common fill device must be protected at the same level as the key it contains.

(5) DTD and SKL can be handled as CCI if the CIK is removed and stored separately.

d. When precautionary supersession is not feasible, several options are available to the CONAUTH. In order of preference, the CONAUTH may—

(1) Extend the cryptoperiod of uncompromised keying material in accordance with doctrinal constraints.

(2) Exclude from net operations those members who do not hold or cannot be furnished replacement material.

(3) Suspend cryptonet operations until key can be resupplied.

(4) Continue to use the compromised key. Caution: This action is a last resort when:

(a) Normal supersession of the compromised material will take place before emergency supersession can be accomplished.

(b) Where keying material changes have a serious detrimental effect on operations.

(c) Where no replacement material is available.

e. The CONAUTH must alert net members (by other secure means if available) that a possible compromise has taken place and direct that members minimize transmissions using the compromised key. Use this option only when continued cryptonet operation is absolutely essential to the mission.

f. The CONAUTH will direct traffic reviews of record traffic encrypted by compromised keying material when warranted.

4–15. Annual reviews

a. CONAUTHs will conduct an annual review of keying material used. Annual reviews must confirm cryptonet structure, membership, quantities, and adequacy of key to meet operational requirements and continuing requirement for the key. The cryptonet must be deactivated if no longer needed.

b. During the review, CONAUTHs must identify large cryptosystems of low peacetime use that are candidates for placement into contingency status.

c. A summary of each review must be sent to USACSLA, NSA, and the appropriate distribution authorities. Special emphasis and efforts will be made towards supporting cryptonets with electronic key and the elimination of hard copy keying material in conjunction with NSA and Army goals of reducing physical key inventories.

4–16. Other functions

a. When a CONAUTH is notified that the Army has granted a waiver to TPI requirements for keying material, the CONAUTH will determine if it is appropriate to notify any or all of the other net members.

b. CONAUTHs will specify key change time for the cryptonet when the time is not prescribed in the keying material. The time selected for crypto key change must have the least operational impact. CONAUTHs may change crypto key change time by notifying the net members.

c. In fixed telecommunications facilities, CONAUTHs will approve the number of extracts of keying material that may be issued to a user at any one time. Protectively packaged hard copy keying material should be issued as entire editions whenever possible. Removing key from its protective packaging defeats the purpose of protective packaging and exposes the key to surreptitious copying.

d. In tactical situations, keying material will be issued in sufficient quantities to support mission requirements. Keying material can be issued in either hard copy or electronic form depending on the risk as determined by the local commander. In high risk environments, key will be issued in electronic form. During actual wartime contingency operations, multiple key storage capacities of the equipment should be used. If equipment does not have multiple fill capacity or has insufficient capacity common fill or approved key transfer devices should be issued.

e. If hard copy keying material is issued, extracts may be issued when only a few settings are required; otherwise the entire edition should be issued. The decision to issue extracts or entire editions should be based on a risk assessment and careful consideration of the logistics problems associated with emergency resupply due to compromise.

f. When large amounts of physical keying material are provided for regular consumption and are destroyed unused, the CONAUTH should consider placing the material into contingency status. Contingency keying material is keying material slated for a specific, yet irregularly occurring, requirement. The material is not activated until needed for the specific requirement and is not destroyed until after use. Substantial savings in production, distribution, accounting, and destruction are realized when contingency materials are used in place of regularly superseded effective key. Any action to establish a contingency cryptonet must be coordinated with appropriate distribution facilities, USACSLA, and NSA.

Chapter 5
Audits, Inspections, and Assessments

Section I
Audits and Inspections

5–1. General
Command COMSEC inspections and USACSLA COMSEC audits and inspections will be conducted as outlined in this chapter. In addition, frequent inspections or checks of the account by authorized personnel are strongly recommended.

5–2. Communications security inspections
USACSLA or the ACOM, ASCC, or DRU command COMSEC inspector or qualified security officer should conduct a COMSEC facility inspection prior to initial activation of any new COMSEC account or a new COMSEC facility, whenever possible. However, such an inspection must be conducted within 90 days of activation. Thereafter, facilities must be reinspected every 2 years or at alternative intervals based on the type of facility, sensitivity of operations, and past security performance.

a. The inspection must address secure operating procedures and practices, handling and storage of COMSEC material, and routine and emergency destruction capabilities of the COMSEC account and selected operational facilities.

b. Relatively small COMSEC accounts and operational facilities consisting of nothing more than GSA-approved security containers, with a limited inventory of holdings and minimal operational activity, may not require the same level of oversight and frequency of inspection as larger accounts.

5–3. Command communications security inspections
The command COMSEC inspection is the backbone of the Army's efforts to ensure that COMSEC material is properly protected. The inspector must ensure COMSEC material is being used, stored, distributed, destroyed, and accounted for under this regulation and TB 380–41. In situations where great distances separate various elements of an ACOM, ASCC, or DRU making command COMSEC inspection visits impractical, the ACOM, ASCC, or DRU should obtain assistance from qualified COMSEC inspectors within the geographical areas.

a. Frequency of command communications security inspections. Command COMSEC inspections will be performed at a minimum of once every 24 months. When an account has failed a USACSLA audit and inspection or a command COMSEC inspection has revealed unsatisfactory practices, the ACOM, ASCC, or DRU will follow-up with a command COMSEC inspection within 6 months to ensure all discrepancies have been corrected and that the account is operating properly.

b. Selection of a command communications security inspector. Command COMSEC inspectors play a significant role in the Army's efforts to protect its COMSEC key and the information it encrypts and/or protects. Command COMSEC inspectors must be selected based on their experience and knowledge of COMSEC policy and procedures. The command COMSEC inspector must be knowledgeable of the COMSEC procedures contained in this regulation and TB 380–41. The command COMSEC inspector must successfully complete the TRADOC-approved COMSEC Account Managers Course, the TRADOC-approved Local COMSEC Management Software Course, and have prior experience as a CAM. Command COMSEC inspectors must meet the unwaived grade requirements for CAMs and be appointed in writing. Command COMSEC inspectors will be either DA civilians or military personnel.

c. Records of inspections. The inspection checklist in TB 380–41 should be used as a guide for command COMSEC inspections. The results of the command COMSEC inspection will be recorded on a formal memorandum report and maintained on file according to AR 25–400–2, until the results of the next command COMSEC inspection are received. A copy will also be provided to the unit commander and the ACOM, ASCC, or DRU G–2. A copy will be provided to USACSLA (SELCL–SAS), Fort Huachuca, AZ 85613–7090.

d. Discrepancies. Discrepancies discovered during command COMSEC inspections must be reconciled within 30

days after receipt of the inspection report. A reply by endorsement will be forwarded to the command COMSEC inspector with a copy furnished to the ACOM, ASCC, or DRU G–2.

5–4. U.S. Army Communications Security Logistics Activity communications security audit and inspections

The formal USACSLA COMSEC audit and/or inspection is the Armywide vehicle to certify and validate central accountability and proper safeguarding and control of COMSEC material. USACSLA will conduct audits and/or inspections of Army COMSEC accounts (to include hand receipts as necessary) under the provisions of this paragraph. COMSEC accounts that hold both CMCS accountable COMSEC material and material governed by CJCSI 3260.01C are subject to USACSLA audits of the Army CMCS accountable material. Auditors will comply with CJCSI 3260.01C and obtain approval from controlling authorities and the commander of the account prior to visiting the account.

a. Frequency of U.S. Army Communications Security Logistics Activity audits and inspections. USACSLA announced audit and inspections will be conducted every 24 months.

b. Notification of audit and inspection. USACSLA COMSEC audits and inspections will be announced approximately 45 days in advance.

c. USACSLA may conduct an unannounced audit and inspection based on security and COMSEC accountability issues. In this case, the Director, USACSLA will provide the audited unit with a memorandum identifying the auditor and inspector(s) and the reason the audit and inspection is unannounced.

d. Detailed procedures, criteria, and reporting instructions are in TB 380–41. Audits and inspections will include a total physical inventory of all accountable COMSEC material charged to the account (to include HRHs) and an examination of the following:

(1) Physical security measures in effect.

(2) COMSEC material management.

(3) Record of the last command COMSEC inspection and USACSLA audit and inspection.

(4) Check of accounting records.

e. Actions prior to audit and inspection. Upon notification of a USACSLA COMSEC audit and inspection, the commander of the unit whose account is to be audited and inspected will ensure the primary and/or alternate CAMs are available during the scheduled audit and inspection. USACSLA will be notified by the commander within 5 working days from initial receipt of the notification if neither the CAM nor alternate will be available.

f. U.S. Army Communications Security Logistics Activity auditors and inspectors. Only qualified personnel who have been certified by the Director, USACSLA as a COMSEC auditor and inspector will conduct USACSLA COMSEC audit and inspections. Certification of both military and civilian personnel is authorized. USACSLA COMSEC auditors and inspectors must meet the unwaived grade requirements for CAMs.

g. Audit and inspection results.

(1) An exit brief will be provided to the organizational commander (or civilian equivalent) responsible for the COMSEC account.

(2) Reports of the USACSLA COMSEC audits and inspections will be forwarded to the command within 45 days of the audit and inspection. Accounts will be rated as either satisfactory or unsatisfactory based on the auditor and inspectors evaluation of all factors involved. Generally, the ratings will be based on the following:

(a) A satisfactory rating indicates the auditor and inspector found both the security and accountability of the COMSEC material to be acceptable even though minor discrepancies may exist.

(b) A rating of unsatisfactory indicates the auditor and inspector found serious problems such as a loss of material, deficiencies that directly impair security of the material, or a loss of accountability for material.

(c) All discrepancies must be reconciled within 30 days of receipt of the audit report and a reply by command memorandum forwarded to USACSLA, with an information copy to the ACOM, ASCC, or DRU G–2. For Reserve and National Guard units, discrepancies will be resolved within 60 days after receipt of the report. The results of the COMSEC audit and inspection will be maintained on file in the COMSEC account until the next USACSLA audit and inspection report is received and results adjudicated.

5–5. Communications security audit failures

The following security measures will be taken for Army COMSEC accounts that have received an unsatisfactory rating on a CSLA COMSEC audit:

a. First unsatisfactory rating. Commands receiving an unsatisfactory rating will be placed on the next fiscal year's audit schedule and must be reinspected by the command COMSEC inspector within 6 months. A memorandum signed by the commander must be received by CSLA no later than 30 days for Active Army units and within 60 days for National Guard and Reserve organizations following receipt of the audit report. The memorandum must state the corrective action(s) taken for all deficiencies identified during the audit.

b. Second consecutive unsatisfactory rating. The following actions will be initiated for COMSEC accounts that receive an unsatisfactory rating for 2 consecutive audits.

(1) Immediate suspension from resupply of physical and electronic key. This will become effective upon completion of the audit and inspection and the suspension will not be lifted until all discrepancies have been corrected.

(2) The account will report corrective actions directly to their respective ACOM, ASCC, or DRU G–2 and CIO/G–6 command inspector.

(3) A memorandum signed by the commander must be received by CSLA no later than 30 days for Active Army units and within 60 days for National Guard and Reserve organizations following receipt of the audit report. The memorandum must state the corrective action(s) for all deficiencies identified during the audit.

(4) If CSLA does not receive the memorandum detailing corrective actions taken within the established timeframes, the audit report will be elevated to the DCS, G–2 for a determination on whether the account should be closed.

c. Third consecutive unsatisfactory rating. Commands receiving an unsatisfactory rating for 3 consecutive audits and inspections will be immediately suspended from resupply of physical and electronic key. CSLA will forward the results of its audit to the DCS, G–2 for a determination on whether the account should be closed.

Section II
Annual Communications Security Assessments

USACSLA will prepare an annual assessment of the state of COMSEC operations within the Army. This report will be derived from the results of USACSLA audit and inspections, COMSEC incident monitoring activities, and any special COMSEC assessments performed during the year.

5–6. Assessment content

Assessment reports covering the calendar year will be available no later than 1 March. The report will be addressed to the Headquarters, Department of the Army, Deputy Chief of Staff, G–2, (DAMI–CDS), 1000 Army Pentagon, Washington, DC 20310–1000 with copies furnished to each ACOM, ASCC, and DRU. The assessment will include the following:

a. Total number of COMSEC accounts in the Army.

b. Number of accounts audited during the year within the U.S. and outside the U.S.

c. Number of accounts that received an unsatisfactory rating and a discussion of the most prevalent reasons for the rating.

d. Discussion of the most common findings in the audits.

e. Command compliance with conducting command COMSEC inspections.

f. Comparison with the previous 2 years to identify any trends.

g. Total number of COMSEC incidents reported during the year within the U.S. and outside the U.S.

h. Number of incidents that resulted in a finding of compromise or compromise cannot be ruled out.

i. Discussion of the most common causes of the incidents.

j. Comparison with the previous 2 years to identify any trends.

k. Recommendations to correct the problems noted.

l. Other information, as appropriate.

5–7. Protective technology inspections

To ensure the integrity of protective technologies, the following inspections will be performed.

a. All personnel who handle or use protectively packaged keying material or tamper-sealed information processing equipment must, upon acceptance, inspect the material for evidence of tampering, and if found, report their findings to the CAM.

b. The CAM will inspect all protectively packaged material upon receipt during each semiannual inventory and prior to opening or removal of the protective technology when required for use or maintenance.

c. USACSLA will inspect protected top secret material at all top secret COMSEC account locations on a random basis so that 100 percent of the accounts will be inspected every 2 years. These inspections may include the use of classified and other special inspection techniques made available by NSA.

d. USACSLA auditors will inspect protectively packaged material during the audit and inspection of all accounts.

Chapter 6
Communications Security Incidents

6–1. General

a. The most damaging COMSEC insecurity is the one that cannot be neutralized because the incident that caused it was not reported. All persons who are responsible for protecting COMSEC material must be able to recognize any incident that has the potential to develop into a COMSEC insecurity and report it to cognizant security authorities.

COMSEC incidents pertaining to classified COMSEC material and cryptographic key will be submitted through COMSEC accounting channels. Incidents pertaining to unclassified COMSEC material, including unkeyed CCI, will be reported by the unit or activity accountable officer responsible for such material.

b. The COMSEC incident reporting and evaluating system allows for the continuous appraisal of security standards for COMSEC material used in the Army and the identification, reporting, evaluation, and investigation of any deviation from or circumvention of these standards.

c. The goal of the COMSEC incident reporting and evaluating system is—

(1) To reduce or eliminate conditions that cause or contribute to COMSEC incidents.

(2) To minimize or negate the adverse effect of COMSEC insecurities.

d. Incidents or insecurities that are unique to a cryptosystem are contained in its specific operational security doctrine, technical bulletins, or in specific DA Pams.

e. All military and civilian employees of the Government, including U.S. Government contractor personnel, have an inherent individual responsibility and obligation to protect COMSEC material. Violations or deviation from the security related provisions of AR 380–40 with regard to the protection and safeguarding of classified and unclassified COMSEC material must be immediately reported to appropriate command and cognizant security authorities. Individuals who discover unattended COMSEC items or become aware of COMSEC material that is not under proper control or physically secured are required to assume custody of that material and protect it from tampering or unauthorized access until it can be transferred to a proper authority.

f. Commanders will report derogatory information, as defined in AR 380–67, on personnel found at fault for COMSEC incidents. The report of derogatory information will be sent to the unit security manager for forwarding through the Joint Personnel Adjudications System (JPAS) to the central clearance facility in accordance with AR 380–67.

g. COMSEC incidents meeting the criteria of paragraph 6–11 will also be reported to the supporting Army counterintelligence office.

h. Any person who knowingly falsifies records or attempts to conceal (cover up) the existence of a COMSEC incident is subject to disciplinary action.

6–2. Reportable communications security incidents

COMSEC incidents will be reported to the Army Communications Security Incident Monitoring Activity (CIMA) at USACSLA, the ACOM, ASCC, or DRU information systems security program manager and, when cryptographic key is involved, to the appropriate CONAUTH. An investigated or evaluated COMSEC incident that has been determined to jeopardize the security integrity of COMSEC material or the secure transmission of U.S. Government information will be declared a COMSEC insecurity. Any COMSEC insecurity that results in the known or presumed unauthorized access to COMSEC material is judged a compromise. The 3 categories of COMSEC incidents that may be determined to be insecurities are physical, cryptographic, and personnel incidents.

6–3. Physical incidents

A physical incident is any loss, or loss of control, theft, capture, recovery by salvage, tampering, unauthorized viewing, access, or photographing that has the potential to jeopardize COMSEC material. Examples are as follows:

a. COMSEC material discovered outside of required COMSEC accountability or physical control.

b. Any instance of insufficient documentation on file to support COMSEC accounting transactions, such as destruction, hand receipting of material (transfers or issues), or return of COMSEC material to the account.

c. The inability to locate COMSEC material that has not been transferred out of the account (for example, “lost” key).

d. COMSEC material left unsecured or unattended, especially where unauthorized persons could have access to it. This includes, but is not limited to, the use of unauthorized locking devices or containers to secure classified COMSEC material. COMSEC material that had been previously reported as properly destroyed when, in fact, the material was not destroyed.

e. Movement of a COMSEC account to a permanent new location without prior submission of a CFAR to USACSLA. This only pertains to COMSEC facilities whose current CFA indicates a room or area as the COMSEC facility. COMSEC facilities that indicate a “safe” as the facility will comply with paragraph 3–5 of this regulation.

f. Other specific incidents which require a formal COMSEC incident report include the following:

(1) Unexplained removal of key from its protective packaging.

(2) Unauthorized disclosure of COMSEC material.

(3) Attempts by unauthorized persons to gain access to COMSEC material.

(4) Receipt of COMSEC material through unauthorized channels.

(5) Material improperly packaged or shipped through unauthorized channels.

(6) Unexplained lack of protective technology or certification labels on equipment.

(7) Damage to inner wrappings on packages.

(8) Destruction performed without a witness or with an improperly cleared witness.

(9) Destruction by other than authorized means.

(10) Conflicting dates recorded by the destruction official and witness upon signing the destruction certificate.

(11) Material not completely destroyed and left unattended.

(12) Unauthorized maintenance of COMSEC equipment. Actual or attempted maintenance by unauthorized personnel or deviation from standard maintenance procedures by certified COMSEC maintenance technicians.

(13) Tampering with, unauthorized modification, or penetration of COMSEC equipment or material.

(14) Deliberate falsification of COMSEC records or reports.

(15) Loss of TPI for top secret keying material.

(16) Failure to establish a no-lone zone, except where a waiver has been granted.

(17) Any loss of control over a keyed fill device.

(18) Activation of antitamper mechanisms or unexplained zeroization of COMSEC equipment when there are indications of unauthorized access or penetration.

(19) Discovery of a clandestine electronic surveillance or recording device in or near a COMSEC facility. This will not be reported as a COMSEC incident until authorized by an investigating counterintelligence (CI) agent, but will be reported in accordance with AR 381–14. Do not report to NSA or USACSLA; only to the supporting CI personnel. All reporting will be classified a minimum of secret and not reported from the facility where the device is found. Prior to the arrival of CI personnel, classify and safeguard information pertaining to any tampering of COMSEC equipment, penetration of protective technologies, or discovery of clandestine devices on a strict "need-to-know" basis. Protect the equipment and store in a limited access area. Take no action until directed by CI personnel. Do not discuss what has been discovered or take any action that might jeopardize evidence or alert suspected perpetrators.

(20) Loss, theft, capture, recovery by salvage, or tampering with keyed or unkeyed CCI equipment.

(21) Loss of a KSV–21 fill card.

(22) Known or suspected tampering of any KSV–21 card. Incompatible keying material between a KSV–21 card and its key tag when discovered during STE association.

(23) The loss of a "user" card with its associated STE.

(24) Demilitarization or disposal of COMSEC equipment through unauthorized channels.

(25) Any other significant occurrence that may jeopardize the physical security of COMSEC material or the information it protects as determined by the cognizant security officer.

g. Exceptions—

(1) If a pen and ink correction is made, and the change in the form is supported by a properly signed and witnessed official memorandum for record that certifies the erroneous entry was an administrative error only and that the destruction was, in fact, properly witnessed, this does not constitute a COMSEC incident.

(2) Production errors and reports of defective keying material are not considered COMSEC incidents; however, they are reportable to NSA for resolution.

6–4. Cryptographic incidents

An equipment malfunction or error by an operator or CAM that adversely affects the cryptosecurity of a machine, automanual, or manual cryptosystem is a cryptographic incident. They include the following:

a. COMSEC keying material that is compromised, superseded, defective, or previously used (and not authorized for reuse), or the incorrect application of keying material, such as:

(1) Use of keying material that was produced without the authorization of NSA.

(2) Use, without the authorization of NSA, of any keying material for other than its intended purpose (for example, use of test key for operational purposes or use of a key on more than one type of equipment). This does not include the use of operational key for training purposes when authorized by the CONAUTH.

(3) Unauthorized extension of a cryptoperiod (any requests for a cryptoperiod extension must be submitted prior to the end of the current cryptoperiod) (see para 4–10).

b. Use of COMSEC equipment having defective cryptologic circuitry or use of an unapproved operating procedure, such as—

(1) Plain text transmission resulting from COMSEC equipment failure or malfunction.

(2) Any transmission during a failure or after an uncorrected failure that may cause improper operation of COMSEC equipment.

c. Use of any COMSEC device, equipment, or algorithms decertified under CJCSI 6510.02D and NSA published Cryptographic Equipment Decertification Memorandum without a system recertification approval. Request for systems recertification approval are covered in CJCSI 6510.02D.

d. Failure to certify or recertify key processors or key generators (KOK–22A and KG–83) as scheduled.

Note. This is not a reportable COMSEC incident when prevented from obtaining routine recertification due to ongoing contingency or combat operations.

e. Discussions via nonsecure telecommunications of details of a COMSEC equipment failure or malfunction.

f. Any other significant occurrence that may jeopardize the cryptosecurity of a COMSEC system as determined by the cognizant security officer.

g. Failure to perform KP changeover.

6–5. Personnel incidents

A personnel incident is any capture, attempted recruitment, known or suspected control by a hostile intelligence entity, or unauthorized absence or defection of an individual having knowledge of or access to COMSEC information or material. Examples are the unauthorized disclosure of COMSEC information or attempts by unauthorized persons to affect such disclosure.

6–6. Regulations governing reporting

a. COMSEC incident reports constitute official command correspondence. They will be submitted by or for the commander. Use direct channels to ensure the report is received within the required time frame. Reports will contain all information required by TB 380–41. Incident reports that involve joint staff positive control material and devices must be addressed in accordance with requirements of CJCSI 3260.01C. Reporting commanders are responsible for notifying their chain of command that a COMSEC incident has occurred.

b. The discovery of possible clandestine intercept devices will be reported under AR 381–14.

c. Suspected deliberate security compromises or possible involvement of foreign intelligence services or foreign national personnel will be reported under AR 381–12.

d. COMSEC incident reports will be classified according to content. Appendix B contains classification guidance. Unclassified reports will be marked FOUO and exempted from automatic disclosure under the provisions of AR 25–55.

6–7. Types of reports

a. Initial report. This report will be submitted for each reportable COMSEC incident. When all the facts regarding the incident are included in an initial report and all the information required by paragraph 6–7*c*, subsequent reporting is not required. In this case, the initial report will also become the final report and will so state. If the initial report serves as a final report, it will include the corrective measures taken or planned to minimize the possibility of a recurrence.

b. Amplifying report. This report will be submitted when there is new information regarding an incident for which an initial report has been submitted or every 30 days until a final report is submitted. It may also serve as a final report.

c. Final report. This report is always required (it may be incorporated into the initial or amplifying report) and must always contain a summary of the results of all inquiries and investigations. This report will include the corrective measures taken or planned to minimize the possibility of a recurrence.

d. Abbreviated reports. During combat operations, abbreviated reports may be submitted to report incidents involving physical security of key. This type of report will give sufficient details to enable the CONAUTH to assess whether a compromise resulted. At a minimum, this type of report must answer the questions who, what, when, where, and how. Where a CONAUTH orders an unscheduled supersession of key as a result of the incident, a subsequent complete formal report will be submitted under this paragraph as soon as possible (see para 6–10).

6–8. Army communications security incident monitoring activity

The Army CIMA, managed by the USACSLA, will—

a. Assign a case number within 24 hours of receipt of the initial incident report.

b. Within 48 hours of receipt of the initial incident report, determine whether the occurrence may have compromised COMSEC material or the information it protects.

c. Evaluate physical COMSEC incidents involving multiple Army CONAUTHs.

d. Evaluate physical incidents involving a single Army CONAUTH when that CONAUTH caused the incidents.

e. Direct additional reporting, as warranted.

f. Have final adjudication authority to determine when a reported COMSEC incident has resulted in a COMSEC insecurity.

6–9. Report precedence and timeliness

a. Message precedence for action addressees and report submission times are indicated below. A lower precedence may be given to information addressees. Reports not submitted within the prescribed time frames will contain an explanation for the delay.

b. Initial reports for the following will be submitted to the CIMA within 24 hours of discovery of the incident, at immediate precedence for action addressees and routine precedence for information addressees.

(1) Currently effective key or key scheduled to become effective within 15 days.

(2) Possible defection, espionage, clandestine exploitation, tampering, or sabotage or unauthorized copying, reproduction, or photographing.

(3) Recently (within 30 days) superseded key.

c. Initial reports for the following will be submitted to the CIMA within 48 hours of discovery of the incident and at priority precedence:

(1) Future key scheduled to become effective in more than 15 days.

(2) Superseded (more than 30 days ago), reserve, or contingency key.

d. Initial reports of any COMSEC incident not covered in paragraphs 6–9*b* and 6–9*c* will be reported within 72 hours of discovery of the incident, normally at routine precedence. However, if the incident has significant potential impact, originators should assign higher precedence.

e. Amplifying and final reports will normally be assigned routine precedence. However, they may be assigned a higher precedence if they contain significant new information that will impact on the evaluation of the incident.

6–10. Reporting procedures during contingency operations or tactical deployments

a. It is recognized that while participating in hostile contingency operations and tactical deployments, circumstances may not permit strict adherence to detailed COMSEC incident reporting requirements. During such periods, abbreviated reports may be submitted for incidents involving keying material where espionage or enemy capture is not suspected. At a minimum, the report must answer the questions: Who, What, Where, When, and How? Abbreviated reports must be submitted immediately and must provide sufficient details to enable the evaluating authority to assess whether an insecurity and compromise has occurred.

b. During actual hostilities, loss of keying material can be life threatening and seriously jeopardize the success of combat operations. Such loss must be reported immediately to each CONAUTH by the most expeditious means so that supersession or recovery actions can be taken. When keying material is lost under combat conditions within 48 hours of its scheduled supersession, a formal incident report is not required provided espionage is not suspected. However, an abbreviated incident report is required following the immediate notification of the CONAUTH.

c. Upon termination of hostilities, major combat commands will prepare summary reports of all COMSEC incidents which have occurred (include those previously reported and those unreported) for submission to the CIMA, DCS, G–2 (DAMI–CDS) and NSA. The summary will list all material lost, dates, places, and a brief description of the circumstances. The report will be classified based on content.

6–11. Counterintelligence reportable communications security incidents

The following are criteria that represent the types of COMSEC incidents that should be reported to a supporting CI agent in accordance with the provisions of AR 381–12. Other incidents that are not administrative in nature may also be reported if there is evidence of foreign involvement. The CI agent will evaluate the circumstances surrounding the incident to assess whether or not it involves espionage or the involvement of foreign intelligence.

a. The available information indicates that the person responsible for the insecurity may have committed a deliberate compromise. An example of this would be the deliberate circumvention of accounting and control procedures.

b. There is evidence that the person or persons involved in the insecurity may be in contact with members of a foreign intelligence service or international terrorist organization.

c. The person or persons involved exhibit behaviors that may be associated with espionage or terrorism as specified in AR 381–12.

6–12. Evaluations

COMSEC incidents are evaluated on the basis of information contained in the COMSEC incident reports and considerations of the security characteristics of the cryptosystem involved. Evaluations are made to determine the effect of the occurrence on the cryptosystem involved. Initial evaluations are made by the CONAUTH and the CIMA to determine the effects of the occurrence. When a cryptosystem has been declared compromised, it will not be used for further encryption unless it is operationally essential to encrypt messages before the supersession date and another suitable system is not available. Evaluations are performed at different levels for different types of incidents (see TB 380–41).

a. Evaluation of a COMSEC incident will result in one of the following determinations:

(1) *Compromise*. This evaluation will be used when material is irretrievably lost or available information clearly proves that the material was made available to an unauthorized person. This will always be declared an insecurity.

(2) *Compromise cannot be ruled out.* This evaluation will be used when available information indicates that the material could have been made available to an unauthorized person, but there is no clear evidence that it was. This may be declared an insecurity.

(3) *No compromise.* This evaluation will be used when information clearly indicates the material was not made available to unauthorized persons. This will not be declared an insecurity.

b. The Army CIMA will monitor and review all COMSEC incident reports involving Army organizations and will make a preliminary determination within 24 hours of receipt of the initial report whether the occurrence may have compromised COMSEC or the information it protects.

c. The Army CIMA will—

(1) Have final adjudication authority to determine when a reported COMSEC incident has resulted in a communications insecurity.

(2) Immediately report the following COMSEC incidents to the DCS, G–2 (DAMI–CDS):

(a) Theft of mission Joint COMSEC Management Office key.

(b) Falsification of records that results in a compromise of COMSEC material.

(c) Any incident that may impact mission critical command, control, and communications operations.

(3) Direct additional reporting, as warranted.

d. The CONAUTH will—

(1) Evaluate COMSEC incidents involving keying material they control, except as specified in the paragraph above. CONAUTHs for communications-electronics operating instructions, joint communications-electronics operating instructions, or signal operating instructions material will evaluate incidents as specified in AR 380–5.

(2) Inform USACSLA of all evaluations.

(3) Initiate recovery actions in accordance with TB 380–41 when they believe material has been compromised.

Note. CONAUTH responsibilities regarding COMSEC incidents are limited to initiating precautionary supersession or other recovery actions as warranted and rendering an evaluation as part of the administrative closure. Related items such as recommending disciplinary action are outside of the CONAUTH's purview.

6–13. Damage assessment

a. The CONAUTH will promptly notify all net members when key is compromised or involved in an incident where compromise cannot be ruled out. In turn, net members will promptly notify all supported commanders that their key has been compromised or subject to possible compromise and that all their communications occurring since that time have been or may have been affected.

b. When a supported commander is notified of a compromise involving key, that commander will determine if and to what degree the compromise affects operations. In making this damage assessment, the commander must consider the type, sensitivity, and classification of information transmitted and the vulnerability of the transmission. Whenever the circumstances dictate, the commander will, as part of the assessment, direct a review of all messages encrypted with the compromised key and take appropriate actions. An overall review of the effects of the compromise should be made at each major headquarters and the CONAUTH should be notified of all conclusions. Information involved in a compromise will not be automatically downgraded or declassified because of the compromise. The classified information contained therein should be reevaluated and downgraded or declassified, as appropriate, under AR 380–5.

c. Compromise of any equipment programmed with COMSEC software and still holding all key splits needed to decrypt that software, while possibly exposing that software to hostile elements, does not automatically necessitate action to supersede the software (for example, replace algorithms). The equipment is protected in various ways to make it difficult for a nonsophisticated adversary to access it. Other protections will be implemented in ECUs to ensure that unauthorized variations of legitimate software are not usable by COMSEC equipment.

d. NSA will evaluate all COMSEC incidents involving STE key. Reports will be addressed to the Director, NSA and to USACSLA.

6–14. Investigations

In certain situations, commanders may determine that an investigation of a COMSEC incident is warranted under the provisions of AR 15–6. If a commander suspects criminal misconduct, it may be more appropriate for the commander to conduct a preliminary inquiry under the Rule for Courts-Martial 303 or to have either the military police or criminal investigation division conduct the investigation. At a minimum, commanders will initiate an investigation for the following types of COMSEC incidents: those involving unexplained or unjustifiable loss of COMSEC material, except that caused by combat or a natural disaster; incidents or situations that appear to be deliberate circumvention of COMSEC accounting and control procedures, including falsification of destruction reports; and those that involve tampering with or the unauthorized modification of COMSEC equipment or key. See AR 735–5 for the loss or destruction of COMSEC equipment. When an AR 15–6 investigation is conducted, the appointing authority for the investigation will make one copy (or a summary) of the report available upon request to USACSLA for use in evaluating the COMSEC incident, as well as, to the appropriate ACOM, ASCC, or DRU headquarters. When individuals are suspected of criminal misconduct involving COMSEC facilities or operations, the commander will suspend their access to cryptographic material pending completion and adjudication of all investigations.

6–15. Relief from accountability

In the event of a COMSEC incident, USACSLA or the CONAUTH will approve relief from CMCS accountability, based on an evaluation of the reported incident. Relief from CMCS accountability will not be construed as relief from property accountability. In all cases, the commander responsible for the account will sign the following certification statement in the COMSEC account incident records: "I certify the circumstances surrounding the loss of (identify the material) have been considered and a determination has been made that a request for relief from property accountability

is or is not required". Relief from CMCS accountability will be obtained in accordance with TB 380–41 (see AR 735–5 for property accountability losses).

6–16. Administrative discrepancies

Administrative discrepancies are considered to be actions that jeopardize the integrity of COMSEC material. Commanders are responsible for ensuring appropriate positive actions are taken to prevent the recurrence of COMSEC administrative discrepancies. The following administrative discrepancies will be reported through the organization's chain of command, as directed by the ACOM, ASCC, or DRU to the cognizant security officer and the CONAUTH.

a. Premature or out-of-sequence use of keying material without the prior approval of the CONAUTH, as long as the material was not reused.

b. Inadvertent destruction of keying material or destruction without authorization from the CONAUTH, as long as the destruction was properly performed and documented.

c. Removing keying material from its protective packaging prior to issue for use or removing the protective packaging without authorization, as long as the removal was documented and there was no reason to suspect espionage.

d. Destruction of COMSEC material or zeroization of a common fill device not performed within required time limits, provided continuous accountability and control prevented unauthorized access.

Chapter 7
Department of the Army Cryptographic Access Program

The DACAP governs the granting of access to U.S. classified cryptographic information that is owned, controlled, and produced by or for the DA.

7–1. Counterintelligence scope polygraphs

In accordance with DODI 5205.08, DA individuals must agree to be subject to a counterintelligence scope polygraph examination to be provided access to classified cryptographic information. DACAP policies contained in this chapter will not alter existing authorities of the Director of National Intelligence under Executive Order (EO) 12333, DODD 5210.48, DODI 5210.91, and AR 381–20. This chapter provides specific procedures for the administration of the DACAP-required CSP Program.

7–2. Program applicability

This program applies to all Army military personnel and civilian employees, including members of the Reserve components and the ARNG; contractors; consultants; and other persons affiliated with the DA whose official duties require continuing access to U.S. classified cryptographic information.

a. For the purpose of this chapter, classified cryptographic information is defined as:

(1) Cryptographic keys and authenticators that are classified as secret crypto or top secret crypto.

(2) The criterion does not apply to confidential or unclassified cryptographic information.

(3) Classified cryptographic media that embody, describe, or implement a classified cryptographic logic, to include (but not limited to) full maintenance manuals, cryptographic descriptions, drawings of cryptographic logic, specifications describing a cryptographic logic, and cryptographic software, firmware, or repositories of such software (for example, magnetic media or optical disks).

b. DACAP applies to the following individuals with cryptographic access, as defined above, and who have the following duties:

(1) CAMs or their equivalents.

(2) Producers or developers of cryptographic key or logic.

(3) Cryptographic maintenance, engineering, or installation technicians.

(4) Supply point employees where cryptographic keying materials are generated or stored and those having access to such materials.

(5) Individuals that secure telecommunications facilities located on the ground, on board ship, or on communications support aircraft and whose duties require keying of cryptographic equipment.

(6) Individuals that prepare, authenticate, and decode nuclear control orders (valid or exercise).

(7) Individuals whose duties require keying of cryptographic equipment.

(8) Individuals with any other responsibility requiring or enabling access to classified cryptographic media.

c. DACAP does not apply to individuals whose duties are to operate (but not key or maintain) systems using cryptographic equipment.

d. The program excludes unkeyed controlled cryptographic items as defined in National Security Telecommunications and Information Systems Security Instructions (NSTISSI) No. 4001.

e. Additionally, this program does not apply to individuals who merely use cryptographic access cards (for example, KSV–21), PINS, and cryptographic ignition keys to access the secure features of secure communications and data transmission devices.

f. In addition, command COMSEC inspectors, staff officers responsible for oversight, and USACSLA auditors are not subject to the DACAP, unless they also subscribe to one of the categories in paragraph 7–2*b*.

g. All Federal agencies requiring the use of cryptographic devices and access to classified cryptographic information are required to have a Cryptographic Access Program. In situations where the Army provides COMSEC support to another DOD element or a non-DOD government agency, the Army CAM providing the material will request a statement from the supported agency verifying that they are in compliance with the cryptographic access requirements of CNSS Policy No. 3. If the CAM is unable to obtain this verification, they will immediately notify the DCS, G–2 (DAMI–CDS) with an information copy to USACSLA (AMSEL–LCA–CAB) and request guidance.

7–3. Conditions for granting access

It is Army policy that a person may be granted access to classified cryptographic information, as specified in paragraph 7–1, only if that person—

a. Is a U.S. citizen.

b. Is a member of the Army, including those assigned to the U.S. Army Reserve or ARNG, a civilian employee of the DA, a DOD-cleared contractor or employee of such contractor, or is employed as a consultant to the Army.

c. Requires access to perform official duties for or on behalf of the DA.

d. Possesses a security clearance appropriate to the level of the classified cryptographic information to be accessed, in accordance with DOD 5200.2–R.

e. Receives a security briefing appropriate to the cryptographic information to be accessed.

f. Acknowledges the granting of access by signing a cryptographic access certificate (see SD Form 572).

g. Agrees to report all foreign travel and contacts in accordance with AR 380–67.

h. Acknowledges, in writing, an agreement to be subject to a CSP examination as a requirement for continuing access to classified cryptographic information.

7–4. Procedures

a. Granting cryptographic access—

(1) The CAM is responsible for advising the commander on who should be granted cryptographic access. The CAM is also responsible for notifying the unit security manager when an individual no longer requires access.

(2) The unit commander is responsible for identifying those personnel requiring cryptographic access (see para 7–2).

b. Cryptographic access briefing (see SD Form 572)—

(1) The unit security manager will be the unit DACAP point of contact and submit initial and update reports to the ACOM, ASCC, or DRU DACAP point of contact any time a person is added to or deleted from the program.

(2) The unit security manager will administer the cryptographic access briefing available in appendix D and prepare the SD Form 572. The security manager will also be responsible for preparing the termination of access portion of the form when an individual's access is terminated for any reason.

(3) The security manager will provide the CAM a list of individuals who have been either enrolled in or terminated from the DACAP.

(4) The signed briefing form (see app D) and the SD Form 572 will be retained in accordance with Army files record maintenance requirements (see AR 25–400–2).

(5) Any individual who refuses to sign SD Form 572, section I will be denied access to all classified cryptographic information.

c. Cryptographic access will be withdrawn whenever an individual is no longer qualified for access to classified cryptographic material. Examples include reassignment to a position not requiring access, termination of employment, suspension of access, or revocation of clearance. Whenever cryptographic access is withdrawn, the individual will be debriefed and will sign the termination of access portion of the memorandum. The security manager will complete the termination of access portion of the SD Form 572.

(1) If cryptographic access is withdrawn as a result of the suspension of an individual's access to classified information, the memorandum will be held in a suspense file until the case has been adjudicated. If an individual's access is suspended due to derogatory information, the information will be reported to the security office for submission to the consolidated Department of Defense Central Adjudication Facility.

(a) If, after favorable adjudication by the Department of Defense Central Adjudication Facility, the commander decides to grant access again, the security manager will brief the individual, prepare and complete a new certification memorandum, and handle it according to paragraph 7–4*b*.

(b) If after adjudication by the Department of Defense Central Adjudication Facility the commander decides not to grant access again, the memorandum with the termination of access portion completed will be maintained according to AR 25–400–2.

(2) If the individual's access is withdrawn for administrative reasons or revoked, the termination of access portion of the memorandum will be completed and the memorandum maintained on file.

(3) Any individual who signs the SD Form 572 acknowledges that they may be randomly selected to undergo a CSP. Any individual who declines to submit to an examination will be denied further access to classified cryptographic information. However, persons denied access for this reason will be retained in a position of equal pay and grade that does not require CSP.

(4) Electronic signatures on cryptographic access briefings are acceptable, provided all legal requirements for authenticity, nonrepudiation, verification, and records management and/or storage are met. The digital signatures must meet the requirements of the National Archives and Records Administration; there must be an apparent included and/or embedded metadata or certificate upon which one could validate or verify the Public Key Infrastructure (PKI) certificates implemented with DA-approved PKI technology and meet the basic DOD and DA PKI verification requirements. Commanders, at all levels who have individuals enrolled in the DACAP will—

(a) Maintain an official roster and database of Army individuals under their command who are enrolled in the DACAP.

(b) Ensure Command Security Officers (for example, S–2, G–2, and/or Security Manager) coordinate with the Army Intelligence Polygraph and Credibility Assessment Program Manager to schedule a random CSP for persons within their command and subordinate commands who are enrolled in the DACAP. Individuals subject to the CSP will be selected, on a random basis, for CSP examinations. The random examination list will be generated on a yearly basis by the ACOM, ASCC, DRU, or ARNG security manager; the names of persons to undergo CSP examination will be

provided, along with a request for CSP support, to the Army Intelligence Polygraph and Credibility Assessment (PCA) Program Manager no later than 1 September of every year. The randomly generated names will be limited to five percent of the individuals who are currently enrolled in the DACAP as of 1 August each year. The list must be generated in such a way as to have no particular pattern, organization, or structure (that is, randomly).

d. See figure 7–1 for an sample of a CSP request.

e. Commanders will ensure that access to all classified cryptographic information under the appropriate command security officer's responsibility is denied or revoked for any individual who refuses to take a CSP examination.

DEPARTMENT OF THE ARMY
OFFICE OF THE DEPUTY CHIEF OF STAFF, G-2
1000 ARMY PENTAGON
WASHINGTON, DC 20310-1000

Your Office Symbol DATE

MEMORANDUM FOR ARMY INTELLIGENCE POLYGRAPH PROGRAM
(IAGX–ACI–PM), 8825 BEULAH STREET, FORT BELVOIR, VA 22060–5246

SUBJECT: Request for Polygraph Examination

1. (U//FOUO) The following individual(s) require a counterintelligence-scope polygraph examination for the following purpose: (reason for exam, that is, program requiring polygraph and DACAP).

NAME	SSN	Rank/Grade	PHONE	ETS DATE
SMITH, Sally A.	555–55–5555	SGT/E-5	703-123-1233	31 Dec 2015
JONES, John B.	000–00–0000	GG13/DB-03	703-123-1233	None

2. (U//FOUO) POC is XXXXXX, phone: XXX–XXX–XXXX, e-mail address: jdoe@us.army.mil.

JOHN A. DOE
(Signature Block of Security Manager)

If your letterhead is different from the above, use yours.
Email address: Contact the U.S. Army Intelligence Polygraph Program Office at 301-677-2497/5456/5394/2734 for current email address.

Figure 7–1. Sample of a CSP request

7–5. Other organizations or agencies

In instances where Army COMSEC key classified top secret crypto or secret crypto is hand receipted to personnel from other Services or DOD organizations, those personnel must be in that Service or organization's cryptographic access program. If it is not considered feasible for them to be enrolled in the program, or if that Service or organization does not have a cryptographic access program, contact DCS, G–2 (DAMI–CDS) for guidance. The same applies to situations where the recipient of the key belongs to a non-DOD organization or activity.

7–6. Scheduling and conduct of command security program examinations

a. The Army Intelligence PCA program manager will—

(1) Task the appropriate INSCOM polygraph element to conduct the CSP examinations based on the names provided by the ACOM, ASCC, DRU, or ARNG command security official.

(2) Determine the number of CSPs that can be conducted based on manpower and resources.

b. The designated INSCOM polygraph element will—

(1) Contact the appropriate Army commanders, supervisors, Army command security officers and contracting officer's representative (COR) to schedule the polygraph examinations.

(2) Be responsible for the polygraph examiner's travel, per diem costs, and other costs directly related to the administration of the CSP examinations.

c. The Government contracting officer's representative at the respective command, and designated in the applicable contract, will arrange for the enrollment of contractor employees through the appropriate ACOM, ASCC, DRU, or ARNG command security office.

7–7. Army commanders, supervisors, and command security officers

The commanders, supervisors, and command security officers will—

a. Ensure all individuals enrolled in the DACAP sign a SD 572 and the Cryptographic Access briefing (see app D).

b. Ensure that any individual with Army cryptographic and COMSEC access who refuses to take a CSP examination, or who is deemed to have refused by being a "no-show" for their third scheduled CSP examination, is denied further access to all Army classified cryptographic information.

c. In coordination with the ACOM, ASCC, DRU, or ARNG command security manager, ensure everyone enrolled in the DACAP is subject to the administration of a random CSP.

d. Individuals enrolled in DACAP who have been notified by their commander, supervisor, command security officer, or contracting officer's representative that they have been selected for a random CSP examination will attend their scheduled CSP examination unless granted an excusal by their commander.

Chapter 8
Controlled Cryptographic Items

This chapter sets forth the minimum standards for controlling unkeyed CCI equipment end items and CCI components. Unless a true distinction is otherwise warranted, henceforth the terms CCI equipment and CCI components will be referred to collectively as CCI. CCIs that contain key will be governed by control requirements set forth in other chapters of this regulation.

8–1. General

CCIs are unclassified COMSEC equipment which contain a cryptographic logic designed to encrypt (encipher) and decrypt (decipher) classified and unclassified communications information. The NSA is the sole Federal Government organization chartered under Federal Statutes and Presidential Executive Order to administer the U.S. Information Security (INFOSEC) Program. As the National INFOSEC Manager, NSA is empowered to develop, regulate, restrict, control, and authorize the manufacture, procurement, production, distribution, use, and final disposition of INFOSEC materiel used by all Federal agencies.

8–2. Purpose

The secure telecommunications and information handling equipment and associated cryptographic components that are designated CCI employ a classified cryptographic logic in their design. The hardware or firmware embodiment of that logic is unclassified but controlled. However, the associated cryptographic engineering drawings, logic descriptions, theory, or operation computer program and related source data remain classified.

a. It is important to note the CCI category of COMSEC materiel fully retains its designation as National Security-Sensitive and must therefore be stringently controlled and accounted for by all persons entrusted with its care and

safekeeping. This chapter prescribes the minimum standards which will be met and adhered to for handling, control, transportation, access, accountability, and reporting of CCI while it is unkeyed. These standards are designed to protect CCI against tampering, unauthorized physical access, and loss of accountability.

b. The control requirements set forth in this chapter are necessary to guard against preventable losses of CCI to an actual or potential adversary. Minor lapses in complying with these requirements should normally be dealt with locally as an administrative action. More serious infractions may be punishable under the various sections of the USC or the UCMJ. Detailed procedures for reporting incidents involving CCI are set forth in this regulation.

8–3. Keyed controlled cryptographic item

When a COMSEC device or other CCI equipment is loaded with cryptographic key (keyed), and when an associated CIK or crypto card is inserted, the device assumes the security classification of the key and materiel or information it is protecting. Keyed CCI will never be handled or processed through the standard logistics system.

a. Individuals who become aware of any violation or deviation to the security-related provisions of this regulation, with regard to the protection and safeguarding of classified and unclassified COMSEC materiel, are obligated to report such conditions to appropriate command and cognizant security authorities immediately.

b. Any person who discovers unattended COMSEC items or becomes aware of COMSEC materiel that is not under proper controls or physically secured is required to assume custody of that materiel and protect it from tampering until it can be transferred to a proper authority.

8–4. Release of controlled cryptographic item equipment

DCS, G–2 (DAMI–CDS) and CIO/G–6 (SAIS–CB) share the responsibility and approval authority for the release of Army-owned COMSEC material (or foreign COMSEC material in Army custody) to nonmilitary agencies, the general public, foreign nationals, or foreign governments. All requests will be submitted through command channels to HQDA with justification.

a. CIO/G–6 has final approval authority for the transfer of Army-owned COMSEC equipment to other military departments. All requests for the transfer of CCI to other DOD elements must be submitted through command channels to the Director, U.S. Army Communications Electronic Command, USACSLA (AMSEL–LCA–IAD). USACSLA will make recommendations to HQDA for approval or disapproval before any transfer action is initiated. The transfer of COMSEC equipment from the Army inventory to other agencies without such approval is strictly prohibited.

b. The CG, TRADOC may authorize the release of CCI to units of the ROTC. Army accounting and reporting policies must be adhered to by ROTC units.

c. CCI may be released for use by appropriately cleared DOD contractors who meet the access requirements of this regulation, as provided for by the Federal Acquisition Regulation and under the provisions of NSA policy. Contract documents must specify procedures for accounting, storage, control, reporting, and the return of CCI to the Army when no longer required or upon termination of the contract.

8–5. System integrated and embedded controlled cryptographic item

The requirements of this regulation also apply to any otherwise unclassified information processing equipment and weapon systems that have been modified through integration of a CCI component. When such equipment is so modified as authorized by NSA, the equipment becomes a CCI in its entirety.

a. Any system that contains an embedded CCI component retains its CCI designation as long as it continues to serve as a host for the CCI integrated cryptographic component. If the CCI component is subsequently removed, the host equipment reverts to its previous status as an unclassified system. Unclassified systems containing an integrated CCI component must be accounted for as CCI and reported under the CCISP per AR 710–3.

b. The installation and removal of CCI cryptographic integrated circuitry within an equipment system is restricted to individuals trained and certified as qualified maintenance technicians for the equipment. In addition, such individuals must have been formally indoctrinated by completion of an NSA-approved Security Awareness Course as certified on DD Form 2625 (CCI Briefing).

c. Removal of exterior covers on equipment to access CCI interior components by individuals who are not certified COMSEC technicians with proper security clearances is a violation of COMSEC security policy and strictly prohibited. Such violations must be reported as a COMSEC incident per chapter 6 of this regulation.

8–6. Protection of unkeyed controlled cryptographic item

Unkeyed CCI will be afforded protection at least equal to that normally provided to other valuable or sensitive material as required by AR 190–51. In addition, the protective measures employed must reasonably guard against attempts by individuals to gain access with the intent of committing acts of theft, sabotage, or tampering.

a. CCI is unclassified but security-sensitive COMSEC equipment used to protect National Defense Information. Absolute access control of CCI is essential because commanders, managers, and users at all levels rely on the security it provides them. They must have total confidence in and be assured of the functional integrity of the various systems and data bases CCI protect. Strict enforcement of accounting policies and procedures, proper handling and storage, and

access control during its operation, shipment, maintenance, or repair, until final disposition of CCI at Tobyhanna Army Depot (TYAD), will ensure the protection afforded to those multimedia and weapons systems by CCI are not jeopardized or degraded.

b. Accountable officers and users are responsible for making sure that CCI contain proper exterior identification at all times to facilitate proper physical control and safeguarding. Whenever CCI labels, tags, data plates containing the CCI caveat, and serial numbers become damaged, illegible, or detached from the equipment immediate action is required to replace them.

8–7. Standard operating procedure for controlled cryptographic item

An SOP will be established and maintained by each Army activity that receives, stores, operates, accounts for, or otherwise handles CCI.

a. The SOP will contain instructions for all pertinent aspects of CCI management applicable to that particular activity, to include the following:

(1) Instructions regarding who may and may not have unsupervised access to CCI.

(2) Physical inspection procedures for signs of tampering or unauthorized access of the different types of CCI handled.

(3) Accounting and inventory procedures.

(4) Measures for safeguarding CCI.

(5) Access control.

(6) CCI operations.

(7) Physical protection of facilities where CCI is housed, operated, or stored.

(8) Packaging and shipment of CCI.

(9) Emergency evacuation or destruction procedures.

(10) Asset reporting per AR 710–3.

(11) The preparation and submission of COMSEC incident reports and administrative incident reports to higher authority as mandated in chapter 6.

b. Commanders must initiate a risk assessment under the provisions of DA Pam 190–51 prior to selecting physical and security protective measures for CCI and document those protective measures in the unit SOP.

8–8. Protection of facilities

Protection will be structured using the applicable provisions of AR 190–51 and by applying the physical protective measures and security procedures being used successfully to protect other unclassified, sensitive, and high-value equipment in similar environments. As a minimum, unkeyed CCI will be afforded the same level of double-barrier protection provided desktop computers in offices, tactical radio sets installed in vehicles, shelters, aircraft, and sensitive equipment in storage.

a. A security-storage structure as defined in AR 190–51 is not required for protection of CCI, except as specified below in paragraph 8–27 for unattended operational sites. Nontactical facilities housing communications-electronic (CE) systems, computer rooms, network components (for example, file servers), and related sensitive areas where CCIs are in operation should be designated as restricted areas and mission essential and vulnerable areas (MEVA) per AR 190–13. Facilities and systems so designated will be included in the installation physical security plan. Periodic physical security inspection requirements are also contained in AR 190–13.

b. Unattended and uninstalled CCI is considered to be in storage when it is in logistics channels and will be safeguarded accordingly. Unattended CCI installed in fixed locations or in mobile or transportable shelters and vehicles are not considered to be in storage and will be provided the same level of protection mandated for similar operational sites.

c. As a matter of policy and recognized prudent security precaution, CCI (keyed or unkeyed) will not be stored in vaults, security containers, or arms storage facilities containing items of monetary value (for example, cash, jewelry, and precious metals), weapons, ammunition, high-pilferable items (for example, binoculars and global positioning systems), or other sensitive items.

(1) Commanders must recognize that each additional item of value stored in a single security storage facility increases the risk of loss by intensifying the target potential to criminal and subversive elements. However, under emergency or tactical contingency conditions, when other secure storage facilities are not reasonably available, commanders may authorize short-term storage (not to exceed 30 days) of CCI in a consolidated secure storage facility.

(2) Long term storage of CCI under these conditions must be supported by a formal risk assessment per AR 190–51 and authorization provided in writing to the accountable officer by a commander O–5 or above in the chain of command.

8–9. Surveillance

With regard to COMSEC operations, surveillance is a methodology which allows for the continuous appraisal of

security standards for the COMSEC materiel used in the Army and the identification, reporting, evaluation, and investigation of any deviation from or circumvention of those standards. The goal of surveillance is—

a. To reduce or eliminate conditions which cause or contribute to COMSEC incidents.

b. To neutralize or minimize the adverse effects of COMSEC insecurities and compromises.

c. Commanders are required to conduct risk analysis and assessments of MEVA as a management tool in allocating resources for the protection of critical Army assets.

d. AR 190–51 and DA Pam 190–51 provide detailed guidance on how to conduct a risk assessment and how often they must be conducted. In addition, AR 25–2 mandates the conduct of risk assessments as part of a risk management plan for information systems security (see AR 190–13 for additional information on MEVAs).

8–10. Handling of controlled cryptographic item

Individuals who do not meet the criteria for access may physically handle unkeyed CCI, subject to both of the following conditions: They are employed by a U.S. Government agency to perform supply and warehouse functions or to transport CCI under the criteria under the direct supervision of a person authorized access.

8–11. Displays, demonstrations, photographing, and marketing of communications security equipment

The public display of classified COMSEC materiel or equipment is prohibited. Requests to photograph classified COMSEC equipment will be submitted to DCS, G–2 for approval.

a. Within the U.S. and its territories and possessions, the public display and photographing of exterior views of CCI in conjunction with official functions and operational routines is permitted, provided adequate controls and safeguards are in place and the equipment is under the constant observation and protection of an authorized individual granted access. Public demonstrations of the equipment in operation must be limited to U.S. citizens or resident aliens granted visual access.

b. The unofficial photographing of CCI end items on display by the general public or visitors at military installations within the U.S. and its territories and possessions may be authorized at the discretion of local commanders, and when such approval is granted, does not constitute a reportable COMSEC incident.

c. The open or public display of CCI equipment at conferences, symposia, meetings, open houses, outside the U.S. and its territories and possessions is forbidden. This prohibition includes public discussion and publication or presentation of information concerning equipment to the general public. Government contractors will comply with NSA/Central Security Service (CSS) Manual 3–16.

8–12. Logistics management of controlled cryptographic item

Army policy requires the management of CCI in the standard logistics system under the provisions of AR 710–2 and AR 725–50. Asset reporting will be accomplished per AR 710–3.

a. This policy applies equally to program managers, program executive officer, and to U.S. Government contractors providing supplies or services under the terms of contracts executed and administered by Army contracting officers. It also applies to Army-owned CCI provided to contractors as GFE.

b. However, COMSEC GFE and materiel owned by other military departments and NSA (including CCI), which is provided on loan to Army contractors for their use, will be accounted for per direction of the owning agency.

8–13. Acquisition of controlled cryptographic item

Program managers, program executive officers, and other agencies or commands who develop or design new systems, and in conjunction with such development, procure standard or nonstandard commercial COMSEC devices to protect their systems, are responsible for compliance with applicable regulations regarding the control of CCI.

a. Based on national policies established by NSA, the acquisition of commercial COMSEC equipment will be strictly controlled. The Army Authorization Document System equipment authorization documents (MTOE, TDA, and common table of allowances) for units programmed to receive new CCI through procurement must be changed accordingly to ensure proper accounting and reporting of CCI devices. Army wholesale managers should be consulted before acquisition or local purchase to confirm that COMSEC items selected for procurement and proposed procurement sources (vendors), have been approved by NSA and HQDA under the Commercial Communications Security Endorsement Program (CCEP) (see AR 710–2).

b. In addition, responsible agencies and commands must coordinate proper cataloging actions by the wholesale inventory manager and LOGSA with respect to assignment of national stock numbers or management control numbers and management codes to include a controlled inventory item code (CIIC–9) to signify the item is designated CCI for accounting, control, and reporting purposes. WARNING: Any agency or individual who introduces COMSEC material into the Army inventory without prior coordination with HQDA and the applicable Army inventory manager and not in compliance with Army COMSEC acquisition policies is in violation of National Security Policy for the control of COMSEC materiel and subject to severe penalties.

8–14. Communications Security Material Control System

The CMCS with its unique COMSEC central office of record and COMSEC accounting infrastructure at depot, retail, and user levels is managed by duly appointed CAMs.

a. CAMs are accountable officers as defined in AR 735–5. These classified accounts are used exclusively to safeguard and administer classified COMSEC materiel and all cryptographic keying material regardless of its classification. Consequently, when cryptographic key is inserted into a CCI, the CCI assumes the classification of the key installed or the classification of the information and data being processed.

b. COMSEC incident reports involving keyed CCI must therefore be prepared by the user and CAM and submitted to the appropriate authorities per chapter 6 of this regulation and TB 380–41.

c. CCI materiel will not be fielded in the CMCS or shipped to an Army COMSEC account. All CCI should be consigned to an installation accountable officer in accordance with standard logistics procedures and marked for the Department of Defense Activity Address Code (DODAAC) assigned to the unit property book account of the intended user and recipient unit identification codes.

d. Certain Army elements performing classified or sensitive operational or test missions and other support functions may require CCI to be controlled within the CMCS to prevent mission disclosure or for other valid reasons. Such circumstances will be documented and requests for waiver to Army CCI accounting policy submitted through command channels to DCS, G–2 (DAMI–CDS) for approval. When such waivers are granted, the USACSLA COMSEC central office of record at Fort Huachuca, AZ will be provided a copy of the approval specifying duration of the waiver.

e. See AR 710–2 for procedures on how to transfer CCI that has been erroneously shipped to a COMSEC account to the appropriate DODAAC account.

8–15. Logistics catalog data

a. Federal logistics catalog data for CCI will be established and maintained by the program manager and Army wholesale commodity manager assigned to support the COMSEC end items or major systems which serve as hosts for embedded CCI components, as identified in the Army master data file (AMDF) and SB 700–20.

b. All CCI and systems containing embedded CCI must be identified with a CIIC–9 and appropriate recoverability and demilitarization codes. In addition, an automatic return item code of S must be assigned (AR 710–1) and the automatic return items list updated to ensure the CCI is returned to TYAD (account W81U11) for final disposition (see AR 710–2).

8–16. Controlled cryptographic item accountability

National policy requires that all CCI Class II and Class VII end items be accounted for on formal accountable property records by serial number and reported to the Army central database managed by the LOGSA. This is accomplished per instructions contained in AR 710–3 under the CCISP. Such records will be used to trace CCI and establish all known locations and owners in the event of loss or a security incident.

a. Quantity accountability is required for uninstalled CCI assemblies and components. These are reportable to LOGSA under the Secondary Item Management System-expanded procedures. Reconciliation of property records for CCI Class IX will only be conducted upon direction of LOGSA. To satisfy Secondary Item Management System-expanded procedures, uninstalled CCI components may only be stocked and managed by automated retail stock record accounts and wholesale managers. Accounting records maintained for CCI at all levels must provide a constant and continuous audit trail for tracking purposes.

b. Uninstalled CCI components are specifically prohibited from stockage below the retail level or on manual stock record accounts. Further, CCI repair parts are not authorized for prescribed load list stockage at the user level or as shop stock by maintenance support activities. However, authorized COMSEC maintenance activities may obtain diagnostic spares on hand receipt from the supporting supply support activity for use in conducting prescribed troubleshooting and testing routines (see AR 710–2).

c. Property book officers will normally receive automatic initial distribution of equipment under total package fielding programs or will be issued new equipment items containing CCI based on a unit requisition and approved The Army Authorization Document System authorization. When PBOs are uncertain how to account for and report CCI items, they should request assistance from their Installation Director of Logistics and immediately contact the appropriate wholesale inventory manager for instructions and guidance, if necessary.

d. Accountable property officers at unit and retail level will comply with the inventory requirements of AR 710–2 for CCI as sensitive items and conduct quarterly inventories. Items reportable under the CCISP must be physically inventoried (sight verified) by serial number. HRHs and other responsible individuals who have CCI in their custody must also conduct sight verification inventories and will be required to provide a written report to the accountable officer documenting the results of the inventory per DA Pam 710–2–1.

e. Accounting, controlled access, and physical security violations pertaining to unkeyed CCI is the responsibility of the commander, accountable property officer, and user. Compliance with chapter 6 of this regulation in reporting COMSEC incidents for CCI is mandatory.

f. Unkeyed CCI will be afforded the same level of secure storage as that provided to other high-value or sensitive unclassified Army assets consistent with the results of risk analysis performed per DA Pam 190–51. When CCI is keyed for operation, the security and control provisions of this regulation and TB 380–41 for classified operations will be adhered to by all users.

8–17. Identification

CCI designated equipment, including host equipment containing embedded CCI, CCI assemblies, and CCI components will be conspicuously identified with the caveat "controlled cryptographic item" or "CCI" markings.

a. Whenever possible, this identification will be accomplished by use of a permanently affixed label or data plate. CCI materiel which does not have a suitable markable surface will be tagged and have the appropriate marking printed on the box or wrapping in which they are packaged by the manufacturer, U.S. Government contractor, depot, or other Government agency. CCI identification tags for such items will not be removed unless required to be removed during installation into host equipment. The host item will then be marked as CCI accordingly for accounting, inventory control, and reporting.

b. Requests for Army-adopted equipment labels and data plates must be submitted through the local installation accountable officer to the source of supply for the equipment identified on the AMDF as the wholesale inventory manager. For commercial COMSEC devices purchased locally under the NSA-approved Commercial COMSEC Endorsement Program, accountable officers may be required to procure replacement data plates directly from the manufacturer or authorized distributor of the equipment. Caution: New data plates must reflect the original serial number assigned to the CCI equipment as reported to LOGSA via the CCISP. Changing serial numbers of CCI equipment is a COMSEC incident reportable to NSA (see TB 380–41).

c. Users who are uncertain about the identification or security classification of COMSEC materiel in their possession should contact their local security managers or the wholesale inventory manager as reflected on the AMDF.

8–18. Turn-in and disposal of controlled cryptographic item

Except as provided for in paragraph 8–18*d*, the turn-in of CCI through Defense Reutilization and Marketing Office (DRMO) channels is a violation of National Security Policy and is prohibited.

a. All CCI, both end items and components, are coded automatic return items and must be returned to the COMSEC Directorate (DODAAC W81U11) at TYAD for final disposal action. This applies to commercial nonstandard COMSEC devices designated CCI as well as to Army adopted standard CCI. Follow the supply procedures contained in AR 710–2.

b. CCI users at property book level must turn-in CCI to the local standard logistics retail support element from which they customarily obtain their supply support to get credit for turn-in and a signed receipt document for posting to the unit property records. Prior technical inspection by a qualified COMSEC technician at the local retail maintenance support element to validate condition, completeness of the equipment, and to ensure the equipment is unkeyed and has not been tampered with is mandatory.

c. Unexplained missing components, evidence of tampering, or the turn-in of equipment in a keyed condition is a reportable COMSEC incident (see chap 6).

d. Retail support elements will dispose of excess CCI in compliance with AR 725–50. Disposition instructions for excess CCI end items do not have to be requested from the source of supply identified on the AMDF via the automated process (see AR 710–2 for shipping instructions).

(1) *Caution.* Regardless of any disposition instructions to the contrary, final disposition of CCI at local retail level activities or through DRMO channels is a violation of National Security Policy. Within the Army, only TYAD is authorized and has the specialized destruction equipment required to completely disintegrate COMSEC equipment in a secure mode.

(2) *Exception.* CE systems, automation equipment, and other weapons systems containing embedded CCI may be disposed of locally through DRMO channels when directed by the wholesale inventory manager.

(a) Such actions will only be taken when authorization and detailed demilitarization instructions have been provided, in writing, by the wholesale inventory manager for the removal of all CCI components and CCI markings (data plates and labels) or other COMSEC markings are removed from the system by authorized COMSEC technicians.

(b) The CCI components and exterior COMSEC and CCI identification markings must be returned to TYAD for disposal. Local disposal actions for CCI may not be taken unless specifically authorized by the assigned wholesale commodity manager.

e. In the event a wholesale commodity manager erroneously directs the disposal of CCI, or major CE, weapons, or information systems containing CCI, locally or through DRMO channels, such instructions will be immediately challenged by the installation accountable officer. When such challenges remain unresolved, a request should be submitted to USACSLA (DSN 879–2332) for additional guidance.

8–19. Access to controlled cryptographic item

The sensitivity of COMSEC materiel requires that strict need-to-know procedures be enforced for access to CCI.

8–20. Access defined

As applied to COMSEC material, access is defined as, "The capability and opportunity of any individual to gain detailed knowledge or possession of COMSEC materiel; or favorable conditions to alter sensitive and classified COMSEC information and materiel".

a. A person does not have access merely by being in a place where COMSEC materiel is kept, provided security measures, physical controls, supervision, and the presence of authorized personnel or escorts deny unsupervised access and the opportunity to penetrate or exploit the COMSEC materiel. Access to CCI that does not conform to the restrictions in this paragraph is a reportable COMSEC incident.

b. A security clearance is not required for access to unkeyed CCI. However, access will be granted by the commander only to persons whose official duties require access and familiarization, that have a need-to-know, and who are one of the following:

(1) U.S. citizens who are members of any branch of the U.S. Armed Forces.

(2) U.S. citizens who are U.S. Government civilian employees or are employed in support of the U.S. Government, such as contractor employees.

(3) U.S. resident aliens who are U.S. Government civilian employees or members of the U.S. Armed Forces.

(4) Authorized foreign nationals.

8–21. Access control

Access control is any reasonable and prudent security measure taken by commanders and other responsible individuals based on local risk assessment to—

a. Control or prevent the capability, ability, and opportunity of any unauthorized individual to have unsupervised or undetected physical contact with COMSEC material.

b. Prevent tampering with or damage to CCI, disrupt operations, subvert or sabotage, gain unauthorized access to its internal components or cryptographic key, or perform unauthorized modification, alteration, or repairs.

c. Access control measures taken should be tailored to local conditions and be consistent with operational priorities. Responsible individuals are encouraged to make maximum use of the professional services available for the conduct of risk assessments by command physical security specialists, INSCOM field representatives, local security managers, and cognizant security authorities in the chain of command.

d. The removal of exterior covers and protective outer casings installed on a CCI device to expose its inner components is prohibited.

8–22. Foreign national access to controlled cryptographic item

DCS, G–2 may authorize certain foreign nationals to have restricted access to CCI, provided such access is granted in accordance with the conditions set forth in this regulation. These conditions apply only to those foreign nationals in countries where the U.S. Government maintains a constant presence and occupies property of the foreign government (for example, a military base, embassy, and consulate).

a. Approval authority for granting access to foreign nationals may be delegated, in writing, to the lowest general officer level (or civilian equivalent) in the ACOM, ASCC, or DRU chain of command. Regardless of the release status of the CCI, foreign nationals may be admitted without escort to areas containing installed CCI when—

(1) The cognizant security authority has determined that the potential risk of tampering with the CCI is acceptable, considering the local threat, vulnerability, and the sensitivity of the information being protected.

(2) Admittance to the area is required in conjunction with building maintenance, custodial duties, or other operational responsibilities that would normally have been performed by unescorted foreign nationals before the CCI was installed in the area.

(3) The CCI is installed in a facility that is either U.S. controlled or a combined facility with a permanent U.S. presence.

(4) The operational security doctrine for the installed CCI equipment does not specifically prohibit admittance to such areas by unescorted foreign nationals.

b. At facilities which are normally manned entirely by foreign nationals, such as storage sites for prepositioning of materiel configured to unit sets or War Reserve, the commander must authorize this access and handling of unkeyed CCI on a case-by-case basis, in writing. A CCI stored in such facilities which is U.S. property and under U.S. accountability will be inventoried quarterly.

c. Prior to allowing foreign nationals who have been granted access to handle CCI under any circumstances, the responsible commander (or equivalent civilian appointee) must complete a formal risk assessment per AR 190–51, DA Pam 190–51, and AR 25–2, when applicable. This assessment must fully consider the potential risk of loss or tampering and document, in writing, their acceptability of that risk.

d. Foreign nationals will not have unsupervised access to keyed CCI. When performing building maintenance,

custodial duties, or other official responsibilities in facilities where CCI is keyed and operational, foreign nationals are permitted to handle CCI provided the requirements of this regulation are satisfied and local SOPs for safeguarding keyed CCI do not specifically prohibit such handling.

Note. A COMSEC device (for example, STE) is not considered keyed when the CIK or crypto card is removed.

e. At facilities where there is no U.S. presence and foreign nationals have unescorted access to keyed CCI, all U.S. distant site locations which communicate with the CCI in that facility must be notified of this foreign national access prior to initiating secure communications or secure data transmissions.

8–23. Access to controlled cryptographic item in logistics channels

a. Foreign nationals will not be appointed accountable property officers for CCI or have unsupervised access to any accounting records for this category of materiel. They will not be permitted to perform any COMSEC or property office functions such as accounting, inventory, or storage of CCI equipment, except as specifically provided for in this regulation. Those functions must be performed by U.S. citizens.

b. Storage facilities which employ foreign nationals as property officers will not be permitted to receive or store CCI materiel.

c. When foreign nationals are employed to perform supply and warehouse functions or to transport CCI, they are allowed to handle CCI. The following restrictions apply:

(1) They must be employed by the U.S. Government or a U.S. Government contractor.

(2) They must be under the constant direct supervision of a person authorized access.

(3) Their duties must be limited to receiving, storing, issuing, or transporting CCI materiel.

(4) The appointed accountable officer must be authorized access.

(5) When transporting CCI, foreign drivers must be accompanied from pickup to drop-off point by a U.S. person who is authorized access to CCI or the materiel must be secured in a locked vehicle enclosure, storage compartment, or other secure storage container from which the foreign driver is excluded access. These enclosures must be locked by a person authorized access and further protected with a serial numbered security shipping seal affixed so that the seal cannot be removed or replaced without a high probability of detection. The serial number of the seal must then be recorded on official documentation to provide evidence of unauthorized access.

d. When foreign nationals are required to issue, transport, or receipt for CCI in the performance of their assigned duties, a person assigned to the activity who is authorized access will review the completed documentation. This individual must ensure that all accounting entries and signatures are valid and that the individual receiving, delivering, or making turn-in of the CCI is properly identified and (in the case of customer transactions) authorized in writing by competent authority to receive or turn-in the materiel (for example, DA Form 1687 (Notice of Delegation of Authority – Receipt for Supplies) signed by the unit commander).

e. Foreign nationals will not have access to inventory records, property accounting records, or any other documents that reflect total on hand quantities of CCI in a geographical area or command or which reveal the location of CCI assets outside of the warehouse or logistics facility where they are employed.

f. Prior to allowing foreign nationals who have NOT been granted access to handle CCI under any circumstances, the responsible commander (or equivalent civilian appointee) will complete a formal risk assessment per AR 190–51 and DA Pam 190–51. That assessment must fully consider the potential risk of loss or tampering and document, in writing, their acceptability of that risk.

8–24. Access by resident aliens

a. In certain situations, access to CCI may be granted to permanently admitted foreign national resident aliens who are civilian employees of the U.S. Government or are active duty or reserve component members of the U.S. Armed Forces. The decision to grant such access will be made by the senior command cognizant security authority based on a determination that the official duties of the resident alien require this access.

b. Permanently admitted resident aliens and any other non-U.S. citizens employed by a U.S. Government contractor or vendor may only be granted access to CCI with the prior written approval of the appropriate NSA program office. Requests for granting such access must be fully justified and must be based on operational need.

8–25. Installation, operation, and relocation of controlled cryptographic item

The installation and operation of CCI equipment at manned sites does not require a vault or USACSLA COMSEC facility approval. However, such operations must be conducted in secure environments where access and observation can be restricted to authorized personnel only and equipment is adequately protected from theft, tampering, surreptitious intrusion, or sabotage. Local facility approvals are at the discretion of the CAM and in accordance with TB 380–41.

8–26. Surveys and risk assessments

A risk analysis performed by cognizant security authorities assigned to local commands is essential for assisting responsible commanders in evaluating operational needs, potential threats to security, formalizing their own risk

assessments, and instituting local policies and procedures to protect and safeguard installed and/or operational and keyed CCI.

a. When there is a valid operational need to install and operate CCI equipment in an unmanned facility in a foreign country or in a facility staffed entirely by foreign nationals, the installation must be approved in advance by the ACOM, ASCC, or DRU command level cognizant security authority. This authority will not be delegated. Unmanned facilities will meet the construction standards mandated for a fixed COMSEC facility and incorporate special control measures specified for unmanned sites, as detailed in TB 380–41. The following limitations also apply:

(1) The CCI equipment must be installed by and remain under control of authorized U.S. personnel who will verify the presence and integrity of the CCI equipment at (unannounced) irregular intervals.

(2) Visits, inspection, and inventory of installed CCI equipment must be performed not less than quarterly.

(3) Those types of installations will employ additional security measures, for example, equipment locking bars, alarms, tamper proof labels, and security containers to prevent and detect unauthorized foreign national access to the CCI equipment.

(4) CCI equipment located in facilities with no U.S. presence may only be keyed with U.S. classified keying materiel by appropriately cleared U.S. personnel. However, keying of CCI equipment with allied or U.S. unclassified keying materiel may be performed by authorized foreign nationals.

b. The senior command cognizant security authority which provided approval for installation at the unattended site will verify the continuing need to retain CCI equipment at those facilities at periodic intervals, not less than every 6 months. The results of such approvals and semiannual reverifications will be documented and retained on file for review by command inspectors and COMSEC auditors.

8–27. Use of controlled cryptographic item equipment in sensitive environments

CCI equipment should not be installed in an environment with an increased opportunity of foreign national access where the risk is unacceptable. If such a move is required to satisfy mission essential operational needs, it must have prior approval of the cognizant security authority.

a. CCI equipment will be thoroughly examined by a qualified COMSEC technician prior to installation and upon removal of the equipment to ensure no tampering has occurred. Upon installation, all available safeguards should be employed.

b. If actual or possible tampering is subsequently detected, the fact must be reported as a COMSEC incident in accordance with chapter 6 of this regulation. The effected equipment will be removed from operational use and secured pending disposition instructions from the Army COMSEC incident monitoring activity or NSA.

8–28. Installation of controlled cryptographic item by foreign nationals

At U.S. manned sites, foreign nationals may be used to install unkeyed CCI equipment, provided—

a. They are under the direct supervision of a U.S. citizen who is employed either by the U.S. Government or a U.S. Government contractor or vendor.

b. Their access is limited to only the external portion of the CCI equipment. They may not perform any installation functions that require access to internal components of the equipment.

8–29. Relocating controlled cryptographic item equipment

CCI used in an office environment or other fixed location may be relocated, with the commander's approval, whenever there is an operational need. Prior to relocation, the equipment should be examined for signs of intrusion or tampering. In the event of such discovery, a COMSEC incident report must be immediately submitted per chapter 6.

a. Use of CCI equipment that is suspected of tampering will be discontinued pending disposition instructions from the Army COMSEC incident monitoring activity or NSA.

b. CCI installed in mobile shelters, vehicles, and other transportable configurations may be relocated as needed to support operational missions or as specified by command operations, plans, and directives. Special precautions and security measures are required when moving keyed and unkeyed CCI between secure locations.

c. The commander's risk assessment must consider the prevalent operational conditions and local risks involved in all relocation plans and act accordingly. Supporting CAMs must be notified of equipment relocations so that local facility approvals can be updated, if a CFA is required by the CAM.

8–30. Emergency protection and destruction of controlled cryptographic item

TB 380–41 provides detailed guidance for the emergency protection, evacuation, or destruction of all COMSEC materiel.

8–31. Emergency plans

Emergency instructions for the protection and evacuation or relocation of CCI contained in COMSEC SOPs and COOP mandated by AR 25–2 should be based upon this general information, consistent with the risks associated to each activity that handles or operates CCI and direction received through command channels.

a. As part of the risk assessment per AR 190–51, a commander (or civilian equivalent) must conduct an analysis of the prevalent conditions in which CCI operations are being conducted and issue guidelines outlining what measures will be taken for the emergency protection, evacuation, or destruction of COMSEC materiel.

b. Responsible individuals must be prepared to continue protecting CCI during an emergency caused by natural disasters, such as flood, fire, civil disturbance, mob actions, or other hostile acts perpetrated by enemy or terrorist attacks. During natural disasters protection should be provided through either evacuation or secure storage.

c. During civil disturbances and other hostile actions, evacuation should be the alternative of choice. However, if this is not possible, destruction may be the only option available to prevent capture of this sensitive equipment or its key.

8–32. Procedures

Emergency procedures must be detailed, in writing, specific, and include the following:

a. Authority for and when the U.S. citizen or resident alien in-charge may implement the procedures.

b. An inventory listing citing the locations of all CCI materiel.

c. Specific evacuation and destruction responsibilities. Identify individuals by position, military occupational specialty, and job title.

d. Location of destruction devices, when applicable.

e. Instructions on how to identify, remove, destroy, and record, in order of priority, the most sensitive installed and spare cryptographic components before destroying the remainder or other CCI materiel and unclassified components.

f. Instructions for recovering and reporting lost or abandoned CCI, to include items "Found On Installation."

g. Requirements for post-emergency inventory of CCI and the submission of COMSEC incident reports.

h. A schedule and procedures for training personnel and for testing the emergency plan.

8–33. Shipment of controlled cryptographic item

CCI must never be packaged for shipment in a keyed condition. Prior to turn-in or preparation for shipment, the equipment must be inspected by a technically qualified and DD Form 2625 certified individual to ensure the equipment is zeroized (unkeyed) and the batteries removed.

8–34. Inspection

Prior to shipment, and upon receipt of a CCI shipment, a thorough inspection of CCI is required to ensure no tampering of the equipment. Any evidence of unauthorized access, mishandling, improper mode of transportation, loss of control while in transit, or other security violation such as shipment in a keyed condition will be immediately reported by the receiving activity or unit to the shipper and a COMSEC incident report submitted per chapter 6 of this regulation.

8–35. Preparation for shipment

Unkeyed CCI will be packaged for shipment in any manner that provides sufficient protection from damage and provides evidence of any attempt to penetrate the package while the materiel is in transit.

a. The package exterior must be marked "CCI" in 2-inch bold letters. Shipping documents will also be clearly marked "CCI" for identification by materiel handlers.

b. CCI shipped as installed equipment in mobile and transportable operational configurations are exempt from the above wrapping and marking requirements.

c. PBOs and other individuals at the user level are required to turn-in CCI to director of logistics or installation accountable officers (supply support activity) or other retail support elements for shipment or other disposal action.

(1) Prior to turn-in by the PBO, CCI must be placed on work request to the designated COMSEC maintenance support facility and technically inspected to ensure the equipment is complete, that it has been zeroized and contains no key material, and when appropriate, batteries are removed.

(2) Upon turn-in to retail accountable officers, PBOs are provided signed receipts for accounting purposes. It is a violation of AR 710–2 supply policy for users to by-pass support elements and ship CCI directly to TYAD. Users that erroneously ship CCI directly to TYAD will not be provided a signed receipt for accounting purposes.

d. CCI will only be shipped to authorized activities and individuals. Packages will be addressed in a manner to ensure delivery of the materiel to an individual who is designated to accept custody for it at the recipient activity. An individual's name will not be used in the address. Rather a functional address designator should be used (for example, an office symbol, duty position or title, or account number (DODAAC)) to ensure proper and timely delivery to the recipient.

e. CCI will not be shipped through CMCS COMSEC account channels. Agencies and commercial vendors who request such shipments through COMSEC accounts will be challenged. When disputes of this nature cannot be resolved at the user level, they will be referred to USACSLA COMSEC policy team (AMSEL–LCA–CPT), DSN 879–6431 or DSN 879–2332 for resolution.

f. Formal transfers of accountability for CCI can only be executed between duly appointed accountable officers administering DODAAC accounts per AR 710–2 and AR 735–5.

8–36. Detailed shipping instructions

a. The shipment and transportation of keyed CCI is specifically prohibited unless the physical configuration and engineering design of the equipment prevents its removal. However, this restriction does not apply to combat or tactical movements or to emergency circumstances when equipment cannot be zeroized based on critical operational mission priorities. Under such circumstances, with full awareness of the inherent risks involved, the commander's discretion will prevail.

b. Electronic fill devices designated CCI may be transported locally by authorized courier personnel with key loaded to satisfy mission operations, provided access requirements are satisfied and adequate safeguards are exercised consistent with existing risk conditions. CIKs will always be removed from such devices before they are transported from one location to another.

c. Fill devices containing top secret key will be protected using TPI controls as mandated by this regulation.

d. The movement of COMSEC fill devices with key loaded to distant locations outside the immediate command geographical boundaries (for example, local installation) must be restricted to mission essential needs, approved by the commander, and shipped via defense courier service or transported by official Government couriers appointed on orders. Such fill devices will be double-barrier packaged as classified materiel and remain in the physical possession of the courier at all times until delivered to and signed for by the authorized recipient. CIKs will not be shipped with the fill device. When couriers are used to escort such equipment, the CIK will be secured and carried separately by the courier.

e. All keyed CCI equipment are considered unclassified for shipping purposes when the associated CIK or crypto card is removed. This is permitted because the device can only be accessed in a secure mode when linked to the CIK. The unauthorized transportation or shipment of keyed CCI with its associated CIK or crypto card is a reportable COMSEC incident.

f. Cellular telephones and other personal electronic devices designated CCI are authorized to be carried and couriered in an individual's personal possession wherever they are required. All individuals carrying such devices on their person should be issued a DD Form 2501. Caution must be taken to protect PINs which access such devices from other individuals.

g. CCI will only be shipped to authorized activities and must be addressed in a manner that will ensure delivery of the materiel to a cleared individual designated to accept custody. Any activity shipping CCI by other than official courier is required to provide advance shipping notice to the intended recipient at least 24 hours prior to the expected delivery date. If a shipment of CCI has not been received by the intended consignee within 5 working days following the expected delivery date, follow-up and tracer action is mandatory.

8–37. Transportation of controlled cryptographic item

The provisions of this chapter do not apply to the shipment of classified COMSEC materiel. Regardless of the mode of transportation selected by shippers or its final destination, CCI must be prepared for shipment as set forth in paragraph 8–35.

a. CCI will only be transported through U.S. controlled channels using a mode of transportation that provides both continuous accountability and reasonable protection against theft or loss of the material while it is in transit.

b. CCI designed and configured for installation within tactical CE and weapons systems may remain installed and transported within the system transporter, shelter, or vehicle, provided the CCI can be adequately protected from damage and secured within (for example, locking bars) and all outer accesses of the conveyance (windows, doors, and canopies) can be secured and locked with high security padlocks and transportation seals to reveal surreptitious unauthorized access.

c. Requests to use a mode of transportation for CCI that is not expressly authorized by this regulation will be submitted through command channels to DCS, G–2 (DAMI–CDS) for consideration and approval.

8–38. Transportation within the United States and its territories and possessions

Any of the following modes of transportation are approved—

a. Authorized U.S. Government or Army couriers.

b. Authorized U.S. Government contractor or company couriers who satisfy the access requirements in paragraph 8–20, as provided for under the terms of Government contracts.

c. USPS registered mail or express mail provided the material does not at any time pass out of U.S. control. When using express mail, the shipper must obtain assurance from USPS authorities that the CCI will receive continuous electronic or manual tracking to the point of delivery.

(1) A recipient's signature must be obtained when using either registered or express mail. With the increased protection and security with privacy, signatures must be protected. CCI packages must be delivered to postal authorities "across the counter" at a USPS facility. Unattended USPS drop points or drop boxes will not be used.

(2) USPS certified or insured mail and first or fourth class parcel post are not approved for shipment of CCI because these USPS mail services do not provide continuous accountability.

d. Commercial carriers who certify they use a system that accurately reflects a continuous chain of accountability for the material while it is in transit. Paragraph 8–40 contains detailed criteria for selection of an appropriate commercial carrier. The shipper is exclusively responsible and will select a commercial carrier based on the carrier's compliance with these criteria. There is no formal listing of approved commercial carriers for CCI.

e. U.S. military or military-contract air service (for example, Air Mobility Command and Logistics Aircraft) provided there is a continuous chain of accountability for the CCI while in transit.

f. Defense Courier Service on a case-by-case basis when there is no other approved mode of transportation servicing a specific destination. Prior authorization must be obtained from the Defense Courier Service before any unkeyed CCI is introduced into the Defense Courier Service System.

8–39. Transportation outside the United States and its territories and possessions

When shipping CCI outside the U.S. and its territories and possessions, the shipping activity will only use those modes of transportation specifically authorized below:

a. Authorized U.S. Government, Service, or agency couriers appointed on orders. Unit couriers conducting local movement of CCI using organic transportation within the immediate command or geographical area do not have to be appointed on orders.

b. Authorized U.S. Government contractors or company couriers who satisfy the access requirements contained in this chapter, as provided by the terms of U.S. Government contracts.

c. USPS registered mail, provided the materiel does not at any time pass out of U.S. control, pass through any foreign postal system, or is subjected to any foreign customs or postal inspection. USPS registered mail may be used to ship unkeyed CCI to or from any overseas location, provided the location is serviced by a fleet post office or Army or Air Force post office that is authorized to process USPS registered mail.

d. U.S. military or military-contract air service carriers (for example, Air Mobility Command and Logistics Aircraft) provided the servicing agency can provide a traceable, continuous chain of accountability and security while it is in transit. CCI materiel shipped to or from locations outside the U.S. and its territories and possessions must remain under continuous U.S. control. Although some limited handling of the CCI materiel by foreign nationals may be unavoidable during aircraft or vehicle loading and unloading operations in foreign countries, the materiel must be returned to U.S. control upon completion of these operations. Should the materiel subsequently show evidence of unauthorized access or tampering, a COMSEC incident report will be submitted as required by this regulation.

e. The U.S. Diplomatic Courier Service should be used when shipping to foreign locations where CCI would be subject to foreign customs or postal inspection or when a fleet post office, Army or Air Force post office, or USPS registered mail services are not available.

f. See paragraph 8–38 for the conditions and criteria under which CCI may be shipped using the Defense Courier Service mode of transportation.

8–40. Transportation of controlled cryptographic item by couriers

When transporting CCI via courier within the U.S., in overseas commands, or to or from foreign locations and the U.S., every attempt will be made to use commercial U.S. flag carriers as the transportation of choice. When this is not possible, the ACOM, ASCC, or DRU cognizant security authority will be notified for permission and assistance in selecting an acceptable foreign flag carrier based on the ACOM, ASCC, or DRU commander's risk assessment.

a. In all instances where CCI is transported overseas using commercial transportation, an itinerary must be prepared in advance for the courier that identifies the specific airline(s) to be used; whether the flight is nonstop or if intermediary stops may be required; the estimated times of departure and arrival; and what foreign customs inspections the CCI may be subjected to in transit.

b. The ACOM, ASCC, or DRU responsible for shipping the CCI equipment may delegate responsibility for reviewing and approving such itineraries to the lowest general officer level (or civilian equivalent) in the chain of command. Further delegation is not authorized.

c. In addition to the required courier orders, instructions, and documentation specified for all couriers above, the overseas courier must also carry any customs documents and clearances needed to permit CCI to enter the destination country and, when necessary, to allow materiel to reenter the U.S. Couriers who may be subject to customs inspection should obtain necessary customs clearance documentation from their cognizant security authority or U.S. State Department (U.S. embassy or consulate) consular officer.

d. Applicable forms issued by the U.S. State Department for this purpose are as follows: (1) Form DSP–5 (Application/License for Permanent Export of Unclassified Defense Articles and Related Technical Data) and (2) Form DSP–73 (Application/License for Temporary Export of Unclassified Defense Articles).

e. The following guidelines will be followed whenever authorized couriers are used to transport CCIs aboard commercial passenger aircraft.

(1) When required by routine airport security procedures, CCIs will be inspected in the presence of Government

couriers. This inspection will normally be limited to external viewing of the CCI. The CCI may be electronically scanned (x-ray) if necessary. However, the equipment covers will not be opened to reveal internal components.

(2) The courier will always carry official documentation that designates the individual as a Government courier and property records that identify the equipment by serial number as security-sensitive property of the U.S. Government.

(3) To the maximum extent possible, CCI will be hand carried by the courier into the passenger section of the aircraft and stowed under constant observation to prevent tampering or theft. However, if the equipment size or configuration is such that the CCI cannot be hand carried into the passenger compartment, the following options should be considered:

(a) If the equipment contains an embedded CCI component installed within an otherwise unclassified end item; where authorized, a qualified COMSEC technician may remove the CCI component from the equipment. The CCI component can then be packaged and hand carried by the courier. The end item minus the CCI component must also be packaged separately to protect it from damage and transported in the cargo section of the conveyance.

(b) If the equipment is designated CCI in its entirety or the CCI components cannot be removed, then it may be necessary to make prior arrangements with the commercial carrier to ensure the Government courier is granted certain considerations (for example, last on and first off the aircraft) and the CCI is afforded special handling. The commercial carrier must ensure that the CCI equipment always accompanies the courier in the event there are transfers in transit between conveyances or changes in itinerary. All reasonable measures must be taken to ensure the courier and the CCI arrives at their final destination at the same time.

f. If a circumstance should occur where the courier and CCI become separated, the courier must immediately notify the commercial carrier representatives so that urgent recovery actions can be initiated. The shipping activity must also be notified and informed of the situation. All facts and circumstances surrounding the separation and loss of control will be documented by the courier. In addition—

(1) When the CCI is subsequently recovered, it must be thoroughly examined for signs of unauthorized access and tampering. If the security seal is still intact and there are no other signs of tampering, the courier will reassume control of the CCI and continue on to the final destination.

(2) However, if the CCI is recovered and it shows signs of unauthorized access or tampering; or if the CCI cannot be located and is considered lost, the shipping activity will initiate a COMSEC incident report in accordance with the procedures set forth in this regulation. When unauthorized access or tampering has occurred in transit, the shipping activity must also provide instructions to the courier on proper handling of the suspect CCI.

8–41. Criteria for selecting a commercial carrier to transport controlled cryptographic item equipment

CCI may be transported by any commercial carrier that warrants in writing to the shipping activity that it can satisfy all of the following requirements.

Note. Commercial carriers cannot be used to transport CCI to foreign destinations.

a. The carrier must—

(1) Be a firm incorporated in the U.S. and provide door-to-door service.

(2) Guarantee delivery within a reasonable number of days based on the mode of transportation selected and destination.

(3) Have a reliable system of tracking individual packages to the extent that should a package become lost, the carrier can, within 24 hours following notification, provide information regarding the package's last known location.

(4) Guarantee the integrity and physical security of the conveyance's contents at all times.

(5) Guarantee that the CCI will be afforded a reasonable degree of protection against theft (for example, use of security lockers or cages, video surveillance, and high security locking devices) should it become necessary for the carrier to make prolonged stops at carrier terminals while in transit.

b. In addition to satisfying the requirements set forth above, the carrier must either—

(1) Use a signature security service or tally record that accurately reflects a continuous chain of custody and accountability by each named individual who takes possession of the package or shipment in transit.

(2) The carrier may use DD Form 1907 (Shipment Signature and Tally Record) or provide its own signature and/or tally record reflecting the required information or use an electronic tracking system that provides an equivalent level of control, custody, and accountability. Delivery records provided to the shipping activity must show the printed name of the individual who receives the CCI materiel at the final destination and that person's official signature.

(3) Information must be available and upon request from a Government representative. The carrier must have a hard copy printout or a readable computerized database that reflects the points where electronic tracking of the package or shipment occurred.

c. In addition to the foregoing, the shipping activity must ensure that documentation accompanying the shipment includes an emergency telephone number and names of individuals authorized to sign for the shipment in the event the carrier attempts to make delivery during nonduty hours.

d. Shipping activities have the sole responsibility for selecting a qualified commercial carrier based on the guidance contained in this regulation and ensuring the carrier's compliance with basic mandatory requirements.

e. COMSEC incidents resulting from the failure of a commercial carrier to comply with these requirements will be reported by the Government entity which discovers the violation (shipper, consignee, or recipient) in accordance with this regulation.

8–42. Transportation of controlled cryptographic item in conjunction with foreign military sales

Policy governing the sale of CCI to foreign governments and international organizations is contained in DOD 5105. 38–M, DOD 5200.1–R, and COMSEC material national policy directives promulgated by the NSA.

a. The AMC foreign military sales case officer must ensure that a transportation plan has been developed for each procuring nation that participates in the COMSEC Materiel Foreign Military Sales Program. The plan will contain specific procedures to be followed when transporting CCI within and outside the U.S. During the transportation phase of the sale, the procuring nation may impose additional security controls beyond those specified by the U.S. which are more stringent than those set forth in this regulation.

b. Within the U.S., the procuring nation may accept delivery of CCI at its own facilities or may designate agents to accept delivery on their behalf at other mutually agreed upon sites. Upon receipt of material delivered to a designated agent or freight forwarder, ownership and responsibility for the CCI material is transferred to the purchasing nation.

c. Unless directed otherwise by the procuring nation, advance notification of the CCI shipment will be sent by the shipping activity to the appropriate recipient activity in the procuring nation.

8–43. Maintenance of controlled cryptographic item

Operator preventive maintenance services and operational test routines may be performed by any individual authorized access to CCI and properly trained using the instructions contained in applicable user level technical manuals.

a. The removal of protective covers and outer casings on CCI equipment to expose inner wiring schematics or cryptographic components is prohibited, except for certified trained CE and COMSEC technicians with appropriate security clearances.

b. Maintenance of CCI equipment by foreign nationals is not authorized, except as provided for below in paragraph 8–47.

8–44. Maintenance facilities

a. The maintenance area used to repair CCI will not be located in a security-storage structure as defined in AR 190–51. However, the area must provide a prudent level of security and double-barrier protection, consistent with a local risk assessment.

b. The responsible maintenance supervisor must have a security SOP for limiting the access and handling of CCI by COMSEC technicians and other authorized persons. The SOP will emphasize that CCI equipment must be inspected to ensure it is unkeyed before it is accepted for repair.

8–45. Certification of controlled cryptographic item maintenance technicians

AR 25–12 provides policy for the training and certification of all CE maintenance technicians performing routine maintenance of COMSEC equipment. Depot level (full) maintenance will only be performed at TYAD by technicians certified on DD Form 1435.

a. U.S. citizen maintenance technicians who are authorized access to CCI must have completed an NSA-approved training course and have been certified by the Army Signal Center at Fort Gordon, GA to perform the level of maintenance on specific items of equipment for which they have been trained. Retention of such certification is dependent on continued proficiency through performance of repair work on the equipment.

b. Only qualified U.S. citizens trained and certified on DD Form 1435 as full or limited maintenance COMSEC technicians are authorized to perform initial inspection (checkout) and maintenance on COMSEC standalone end items or on those sections or components of equipment and systems that contain a COMSEC (cryptographic) embedded CCI device.

c. Per AR 25–12, all electronic maintenance technicians must also receive formal security awareness training on COMSEC equipment. As a minimum, training will be provided by technically qualified security specialists or COMSEC technicians or instructors on COMSEC doctrine, policy, security threat awareness, and awareness of protective technologies, when appropriate. Completion of security awareness training does not authorize electronics technicians who are not certified COMSEC technicians to perform maintenance on standalone COMSEC equipment or cryptographic (CCI) components.

d. Security awareness training will be recorded on DD Form 2625. This record will be used by command inspectors to verify that training has been received, therefore a copy should be placed in personnel files, a copy retained on file at the maintenance facility, and a copy provided to the individual.

e. A security awareness training package has been developed by NSA and made available for use to DOD and DA training activities. ACOMs may request copies of the program of instruction from the Director, Ordnance Electronic

Maintenance Training Department (COMSEC Account 5P3364), Fort Gordon, GA, DSN 780–2913 and DSN 780–5118.

8–46. Controlled cryptographic item maintenance policy

When a system containing embedded CCI components is turned in or retrograded to a designated maintenance facility or depot for repair or overhaul, the following security measures must be taken:

a. Prior to any work being performed on the system, the CCI components will be removed from the host equipment by an authorized maintenance technician as the first step in the system overhaul process, placed in secure storage, and safeguarded. Such removal will be documented on the work order and the CCI component serial number recorded.

b. Upon completion of maintenance services to the system, the CCI component will be re-installed in its host equipment for final quality assurance test and return of the complete system to the user or secure storage, as applicable. Such actions are necessary to prevent the loss or unauthorized tampering of sensitive CCI components.

c. Failure to take appropriate measures to safeguard CCI components which result in unrestricted access by unauthorized individuals will require submission of a COMSEC incident report per chapter 6 of this regulation.

8–47. Maintenance of controlled cryptographic item by foreign nationals

a. Foreign nationals may be used to perform limited maintenance on CCI equipment when they are under the direct supervision of a U.S. citizen who is employed either by the U.S. Government, a U.S. Government contractor, or vendor authorized to perform maintenance. Approval must be granted in writing by the senior commander in the chain of command.

b. ACOMs, ASCCs, or DRUs may authorize foreign nationals to perform limited maintenance on CCI equipment, provided all of the following conditions are satisfied. The foreign nationals—

(1) Must be employed by the U.S. Government, a U.S. Government contractor, or vendor.

(2) Must be citizens of a country to which the CCI equipment to be maintained has been formally released by NSA.

(3) Must successfully complete an NSA-approved limited maintenance training course for the equipment. In addition those individuals must have received security awareness training. DD Form 2625 will be retained on file for all foreign national maintenance technicians.

(4) Must not require access to classified information or material; or otherwise must be appropriately cleared, having been granted limited access authorization to such classified COMSEC information in the performance of their duties.

(5) Must restrict their maintenance capability to direct replacement of CCI components. Foreign nationals who qualify under this criterion may perform all levels of maintenance on unclassified systems, but only limited maintenance (removal or installation) of the embedded CCI-designated components.

c. Foreign nationals will not perform any repair work on CCI components or the COMSEC portion of CCI equipment.

d. Whenever maintenance of CCI equipment is performed entirely or in part by foreign nationals the equipment will be inspected and fully tested by a qualified technician prior to returning the equipment to service. This technician must be a U.S. citizen who is capable of detecting any unauthorized modifications to the CCI equipment or a CCI component.

8–48. Modification of controlled cryptographic item

Refer to specific equipment maintenance manuals for information on applying modifications.

a. Except as provided for in official NSA and HQDA publications, the modification of classified COMSEC equipment and CCI is specifically prohibited. Any individual who attempts to alter or tamper with COMSEC materiel is subject to administrative and civil sanctions, including adverse personnel actions as well as criminal sanctions under the UCMJ and/or Federal law, as appropriate.

b. The authorized and directed modification of Army COMSEC equipment is routinely performed at TYAD and other designated special repair activities as provided for in officially published NSA and DA modification work orders.

c. In emergency situations, supporting classified missions or other high priority contingency operations, a nonscheduled field modification may be directed by HQDA and performed by specially trained authorized individuals onsite.

d. In the event a field modification is performed to a common item of equipment (not previously designated CCI) to provide it a cryptographic capability, the following guidance is provided:

(1) When information processing equipment or communications equipment has been modified through integration of a CCI component, the equipment becomes a CCI in its entirety.

(2) Normally the CCI component is embedded within the host equipment and is not readily identifiable or visible for inventory purposes by the user. For this reason, the serial number of the host equipment is used for accounting and reporting purposes.

(3) A label will be affixed to the host equipment to conspicuously identify it as CCI. In addition, the label will reflect identifying information regarding the embedded CCI component.

(4) See TB 380–41 for instructions on how to obtain a CCI label.

(5) Modified equipment will be immediately reported to the accountable officer (PBO) for administrative adjustment of property records and CCISP reporting using procedures contained in AR 710–3.

(6) Modified equipment will be physically safeguarded as provided for in this regulation for CCI, inventoried, and accounted for as a sensitive (CCI) item, so long as it continues to serve as a host for the CCI component.

e. If the CCI component is subsequently removed per direction of competent authority, the host equipment reverts to its previous status as an unclassified (non-CCI) common end item and is reported as a loss to the CCISP database accordingly. All labels identifying the item as CCI must also be removed. Individual item accountability for the removed CCI component will be reestablished immediately upon removal from the host equipment by the responsible retail or wholesale accountable officer.

Note. Host equipment will never be opened by unauthorized individuals for the sole purpose of verifying the presence of integrated CCI components.

8–49. Incident reporting

Violations of National Policy in the control, accounting, and protection of CCI materiel will be administered and reported as directed in chapter 6 of this regulation. COMSEC incidents pertaining to keyed CCI must be reported through CMCS channels.

8–50. Communications security incident and administrative incident reporting

National policy mandates that each Government department and agency designate a single central authority to provide oversight for the management of CCI assets held by the department or agency. Within DA, this HQDA staff mission has been assigned to the DCS, G–2.

a. USACSLA is the Army wholesale commodity manager for all centrally managed COMSEC material. Within the scope of this worldwide mission, USACSLA serves as the Army COMSEC central office of record. As such, that activity has been chartered by HQDA as the Army agency for administration of the COMSEC Incident Reporting System and incident adjudication authority.

b. All Army COMSEC incidents which require reporting beyond command levels will be processed, evaluated, and adjudicated by the USACSLA CIMA to determine whether or not they are COMSEC insecurities. Detailed instructions for reporting COMSEC incidents are contained in chapter 6 of this regulation and TB 380–41.

c. A COMSEC insecurity is any investigated or evaluated incident which has been determined to jeopardize the security integrity of COMSEC material or the secure transmission of Government information. Any COMSEC insecurity that results in the known or presumed unauthorized access to COMSEC material is judged to be a security compromise and must be dealt with accordingly.

8–51. General

This paragraph prescribes responsibilities and procedures for reporting COMSEC incidents involving unkeyed CCI only. Incidents involving keyed CCI will be immediately reported to the local security authority and supporting CAM for submission of a COMSEC incident report through CMCS channels per TB 380–41.

a. The commander (or civilian equivalent) in physical possession of the COMSEC material involved in a COMSEC incident is responsible for the submission of a COMSEC incident report. Therefore, it is the commander who must finally decide what element or individual in the command will actually prepare the report. That element or individual must have the full support, cooperation, and assistance of other knowledgeable persons in compiling facts and circumstances and preparing COMSEC incident reports.

b. Normally incident reports for classified COMSEC equipment, COMSEC key, and for keyed CCI are prepared by the CAM, as the person accountable for classified COMSEC materiel and cryptographic key. Logically then, incident reports for unkeyed CCI should be prepared by the unit PBO or the installation accountable officer (when applicable), as the person accountable for CCI.

c. Any person, regardless of the position, mission, or assigned duties, who discovers or has knowledge of the loss, tampering, mishandling, unauthorized access, or possible compromise of COMSEC material will immediately take custody of the item, safeguard it, and report the circumstances to the unit or activity security officer and the commander.

d. The commander who has custody of the COMSEC materiel must then decide on the appropriate course of action based on established policy and procedures. The preparation and submission of a COMSEC incident report and conduct of a formal investigation is mandatory, even if ownership of the materiel cannot be readily determined.

(1) Generally speaking, any incident of physical loss or loss of access control for unkeyed CCI under known, unknown, or unexplainable circumstances will be reported. Insignificant lapses in carrying out minor administrative procedures where unauthorized access is improbable will be evaluated by local security managers and reported through command channels only as an administrative (COMSEC) incident for appropriate corrective action to preclude recurrence.

(2) In all instances where unauthorized access, tampering, or compromise is suspected by competent authority to

have been possible or a determination of improbability cannot be ascertained to a reasonable degree of certainty, a formal COMSEC incident report will be submitted per chapter 6 for final evaluation.

e. The submission of a COMSEC incident report for CCI that has been lost, damaged, or destroyed is a security-related mandatory requirement. However, it does not satisfy property accounting policies established in AR 710–2 or AR 735–5. In addition to the immediate submission of a COMSEC incident report by the responsible individual, Army accountable property officers will process appropriate property adjustment documents as provided for in AR 710–2 and 735–5 whenever CCI is lost, damaged, or destroyed through other than fair wear and tear.

8–52. Investigations

Normally, informal commander inquiries about reportable COMSEC incidents will uncover sufficient information to determine whether or not an insecurity and potential compromise has occurred and indicate measures necessary to prevent recurrence.

a. As a result of initial inquiries, commanders may determine that a formal investigation of a COMSEC incident is warranted under the provisions of AR 15–6. This is not always a commander's decision. AR 735–5 mandates an AR 15–6 investigation for all physical losses of CCI.

b. When such an investigation is conducted, the appointing authority for the investigation will make a copy (or a summary) of the final investigation report available to the Army CIMA (USACSLA) upon request, as well as, the appropriate major command headquarters.

8–53. Evaluations

COMSEC incidents are evaluated and adjudicated on the basis of information contained in the COMSEC incident report and consideration of the cryptographic security characteristics of the CCI equipment involved.

a. Evaluations are made to determine the effect of the security violation on the equipment, the classification of the information it was processing, and its potential impact to National Security. See chapter 6 of this regulation for details.

b. USACSLA, as the Army CIMA, will monitor and review all reportable COMSEC incident reports involving Army organizations and activities. USACSLA will have final adjudication authority on such incidents and make determinations as to when a reported COMSEC incident has resulted in a COMSEC insecurity. NSA or USACSLA may also direct additional reporting as warranted.

8–54. Command action

Commanders must consider appropriate disciplinary action for any individual who—

a. Is found to have acted in flagrant disregard of Army COMSEC policy.

b. Fraudulently alters CCI accounting or control records.

c. Is guilty of gross negligence in the protection and control of COMSEC material.

d. Knowingly and willfully fails to report a violation of Army COMSEC policy or procedures, thereby concealing a reportable COMSEC incident.

8–55. Reportable communications security incidents

A reportable COMSEC incident is an occurrence that violates COMSEC policy and potentially jeopardizes the security of COMSEC material or the security and protection of national security information.

a. Controlled cryptographic item is unclassified. However, when CCI is loaded with cryptographic key, it must be protected in a manner consistent with the classification of the key and information it processes. Incident reports involving keyed CCI will be prepared accordingly and submitted per TB 380–41.

b. Types of reportable controlled cryptographic item incidents. The following incidents will be reported per chapter 6:

(1) A determination that a CCI cannot be accounted for and may be lost.

(2) Quantity variations between the physical inventory count of an organization or activity accountable property record and the on hand physical inventory count when the variation cannot be reconciled through recount, causative reconciliation of supporting record files, or otherwise legitimately attributed to simple administrative error.

(3) CCI "found on installation" and unaccounted for.

(4) Where as a result of an initial investigation, cognizant security authorities make a determination that unauthorized access, tampering, or compromise of CCI cannot be ruled out or certified as improbable.

(5) Any incident resulting in the actual or possible circumstance or evidence that an unauthorized individual gained access, tampered with, or modified CCI.

(6) Discovery of missing internal components to a CCI end item or missing parts to a CCI component assembly.

(7) Actual or suspected theft of a CCI.

(8) Transportation or shipment of CCI in a keyed condition. Any instance where a CCI has been shipped in other than a zeroized or unkeyed condition, unless the shipping activity requested and received (prior to shipment) a written waiver to Army COMSEC policy from DCS, G–2.

(9) Deliberate falsification of COMSEC control documents or accounting records.

(10) Unauthorized release of CCI to non-U.S. Government agencies.

(11) Covert or surreptitious attempts by unauthorized individuals to obtain a CCI device or to acquire knowledge regarding its operation, functions, physical construction, or electronic and cryptographic characteristics.

(12) Improper destruction or disposal of CCI.

Note. All CCI must be returned to TYAD for final disposal or destruction. The turn-in of CCI to DRMO is specifically prohibited.

(13) Any maintenance or service routines by an unauthorized person or unauthorized modification.

(14) Unauthorized sketches, drawing, photographing, photocopying, or similar graphic reproduction of CCI equipment internal components. Such actions are specifically prohibited.

(15) Transportation of CCI by other than authorized modes which result in suspected tampering or unauthorized access.

(16) Any other occurrence or CCI incident which a responsible security authority determines may have jeopardized the security of COMSEC materiel or the information it protects.

c. Reporting timeframes and precedence are specified in chapter 6. Multiple reports on a particular incident are normally filed in sequence, each relating additional information as the incident investigation proceeds until a final report is provided.

8–56. Contents of reports

COMSEC incident reports constitute official command correspondence. They must be submitted by or for commanders under their signature or that of a designated senior command staff member. Detailed instructions and a sample COMSEC incident report can be found in TB 380–41.

a. In order to conduct a proper evaluation, it is vital that all immediately available and essential information be included in the initial report concerning CCI incidents. Reports will not be delayed for reasons of obtaining additional information. To minimize time delays, COMSEC incident reports must be transmitted by available electrical modes. Memorandum reports may be used only when electrical means are not available.

b. The initial report will be classified in accordance with chapter 6 of this regulation based on the sensitivity of the information it contains and is normally filed in message form. Use direct channels to ensure the report is received within the required time frames.

c. COMSEC incidents meeting the criteria of paragraph 6–11 will be reported to the supporting Army CI office in accordance with AR 381–12.

d. The amplifying report is normally filed in message form. Classify according to content. This report is used to provide additional information missing from the initial report and will be submitted every 30 days as an update until a final report is submitted. This report is also used to immediately convey significant new information discovered about an earlier reported incident, even if a final report has been submitted and final adjudication action had previously been taken by the cognizant authority.

e. A final report is always required; however, it may be incorporated into the initial or amplifying report. This report is also filed by electrical message and classified according to the sensitivity of the information it contains. Contents of the final report will include the following:

(1) A summary of the results of all inquiries and investigations, including financial liability investigation of property loss and AR 15–6 proceedings.

(2) The local security authority's final evaluation of the COMSEC incident and an assessment as to whether unauthorized access is considered possible, probable, certain, improbable, or impossible.

(3) Final conclusions and corrective measures taken or planned by the commander to prevent a recurrence of such incidents. In the summary portion of the incident report, describe all corrective actions taken by the commander to preclude a repeat of the incident in the future. Provide a point of contact by name with a complete commercial or DSN telephone number and email address, when available.

Note. When it is possible to include all facts in an initial report, identify the report as an initial and final report and subsequent reporting is not required. However, when all information is not immediately available, it may be necessary to submit a fragmentary initial report to meet the imposed time frames and provide supplementary information via an intermediate amplifying report. Do not delay the submission of initial reports beyond the time frames cited in chapter 6 for any reason. Failure to submit a timely COMSEC incident report is a security violation in and of itself for which commanders will be held personally accountable.

8–57. Reportable administrative (communications security) incidents

Administrative COMSEC incidents are infractions of established policies and procedures which are not as serious as those cited in paragraph 8–55, but are considered actions which jeopardize the integrity of COMSEC materiel.

a. The following administrative incidents will be reported through command channels only, provided there is no suspicion of unauthorized access or tampering is determined by competent authorities to be improbable:

(1) Transportation of CCI by means or under circumstances not specifically authorized in this chapter.

(2) Movement of CCI without proper documentation or with documentation which contain significant errors.

(3) Turn-in of CCI to DRMO or other unauthorized activity, and its subsequent recovery.

Note. If CCI is turned-in to DRMO and is not recovered before disposal action is taken or evidence of tampering while in DRMO channels is discovered, a formal COMSEC incident report must be initiated per paragraph 8–55.

(4) Variations in equipment serial numbers, make or model, between information recorded on accounting records and reported to the CCISP and equipment physically on hand, which cannot be reconciled through causative research of supporting record files or otherwise legitimately attributed to simple administrative error. If there is any evidence of fraud, falsification of accounting records, equipment diversion, "swapping," or other serious violation of COMSEC policy, refer to paragraph 8–55.

(5) Failure to provide adequate control and physical security protection for CCI per guidance provided in AR 190–51 and this regulation.

(6) Receipt of CCI with missing external components, accessories, data plates, or CCI labels.

(7) Receipt of a package containing CCI where the package was not annotated as required by paragraph 8–35.

(8) Failure of the shipping activity to provide advance shipment notification as required by this regulation.

(9) Any other administrative infraction to the policies and procedures for CCI which a responsible security authority determines may have jeopardized the integrity of CCI materiel.

b. Reports pertaining to administrative (COMSEC) incidents will be prepared and submitted within 5 working days after discovery. Administrative incidents may be reported by message or memorandum as official correspondence. They are exempt from reports control symbol requirements.

c. There is no specific format for this type of report. However, it should contain detailed information and include all pertinent facts and circumstances necessary for commanders to evaluate and make a final determination on appropriate corrective action. Reporting agencies may use the general format for incident reporting contained in TB 380–41 as a guide, at their own discretion.

d. Reportable administrative incidents discovered by agencies and activities, which pertain to CCI procedural violations committed by other commands, will be submitted to the respective senior commander above the offending organization for appropriate action with an information copy to the responsible unit or activity.

e. Administrative (COMSEC) incidents will not be classified except when justified based on information content. Unclassified administrative incident reports will be marked "FOR OFFICIAL USE ONLY" and exempted from automatic disclosure under the provisions of AR 25–55.

f. The command evaluation of COMSEC material management by CAMs and PBOs, and the review of incident reports is an important function of command inspectors. In addition to the more serious incidents reported to USACSLA, commanders must take note of the administrative (COMSEC) violations committed by elements of their command and recognize them as practices dangerous to the integrity of COMSEC materiel. Quite often these minor infractions are indicators of a need for additional training, or laxity in control of COMSEC materiel at the user level and could result in more serious incidents if corrective action is not taken.

g. The preparation and submission of administrative (COMSEC) incident reports within the chain of command provides all commanders oversight and a system of checks and balances for evaluating shortcomings in operational procedures. Most of the time these minor incidents occur because of inadequate training or supervision, failure to adhere to established SOPs, or a lack of specificity in the SOP itself. Whatever the reason, such reports of violations to established policy must not go unattended.

h. Intermediate commanders in the chain of command must ensure incident reports are administered and that appropriate action is taken if a unit is found to have committed a COMSEC violation. Intermediate commanders must also ensure timely written replies are provided by endorsement to all interested parties, detailing specific actions taken to preclude a recurrence. Repeated violations within a subordinate command element may signal the need for more aggressive remedial action by senior commanders.

i. Reports of administrative discrepancies received from agencies and activities in other commands should, as a matter of courtesy, be responded to in a timely and positive manner with a brief explanation of actions being taken to preclude such errors in the future.

Chapter 9
Emergency Protection of Communications Security Material

9–1. Emergency planning

All COMSEC accounts must have an emergency plan. Planners need to consider natural disasters such as fire, flood, tornado, and earthquake and hostile actions such as enemy or terrorist attack, mob action, and civil disturbances. For natural disasters, planning will usually be oriented toward secure storage. Planning for hostile actions and civil disturbances will usually consider actions to effectively evacuate or destroy the COMSEC material (see TB 380–41 for detailed instructions). Each plan may vary according to the geographic area involved. The reduction or elimination of physical COMSEC material, to include keying material, will facilitate any emergency planning.

9–2. Planning for disasters

Emergency plans must take into account the possibility of natural disasters (for example, floods and earthquakes) and man-made disasters, such as fire and explosions. Effective planning must provide for—

a. Fire reporting and initial fire fighting by persons on duty. In most cases, this will be a part of the normal fire emergency plan for the building that houses the account and need not be prepared as a separate document.

b. Assignment of on-the-scene responsibility for ensuring access control of all COMSEC material.

c. Securing or removing COMSEC material and evacuating the area.

d. Access control of material when emergency crews are admitted into the area.

e. Assessing and reporting probable exposure of COMSEC material to unauthorized persons during the emergency.

f. Access to the LMD and/or KP workstation.

g. Post-emergency inventory of COMSEC material and reporting of any losses or unauthorized exposures.

9–3. Planning for hostile actions and civil disturbances

These plans must take into account the types of situations that might occur, such as an ordered withdrawal over a specified period of time, an unstable political environment where destruction must be done discreetly to avoid adverse reactions, or situations where being overrun by a hostile force is imminent. Such planning must provide for the following:

a. Assessing the risk and probability that various types of hostile actions might occur and the threat these potential emergencies could pose.

b. Availability and adequacy of physical protective measures, such as perimeter controls and physical defenses for fixed, mobile, or transportable facilities where COMSEC material is being used.

c. Security procedures and the assets to affect evacuation of COMSEC material under emergency conditions, including an assessment of the probable risks associated with evacuation. Except when there will be an urgent need to restore secure communications after relocation, key should be destroyed rather than evacuated.

d. Destruction facilities and procedures for affecting secure emergency destruction of physical COMSEC material, including an adequate supply of destruction devices, electrical power, adequately protected destruction areas, and sufficient personnel.

e. Electrical power for destruction of electronic key.

f. Precautionary destruction of COMSEC material, particularly maintenance manuals and key, which are not operationally required to ensure continuity of operations during the emergency. In a deteriorating situation all full maintenance manuals should be destroyed. When there is not time under emergency conditions to completely destroy such manuals, every reasonable effort must be made to remove and destroy the sensitive pages containing cryptographic logic.

g. Emergency procedures should be planned for establishing external communications. Communications should be limited to the minimum necessary. When there is warning of hostile intent and physical security protection is inadequate to prevent a hostile take over of the facility, secure communications should be discontinued in time to do a complete destruction.

9–4. Preparing the emergency plan

The CAM should prepare the emergency plan. If the plan calls for destroying the COMSEC material in place, all emergency destruction material, devices, and facilities must be readily available and ready to use. If the plan calls for emergency evacuation, a location must be identified and a route or routes mapped out in advance and transportation arranged for. The plan must be realistic and workable and must address all goals. It must agree with or be a part of the command, installation, or activity basic emergency plan. The following must be included for an effective plan:

a. Clearly and concisely describe duties. Everyone must understand the plan and be able to implement and perform all actions.

b. Provisions for secure storage, evacuation, or destruction of all COMSEC material. Planners must consider which of these options may be applicable to their facility, either alone or in combination.

c. In those instances where the plan calls for actions that require resources in addition to those within the COMSEC account, the CAM must ensure that coordination has been performed and written agreements are in place as necessary (for example, to secure a vehicle and for storage space at an alternate location).

9–5. Rehearsing the plan

a. The plan should be rehearsed frequently to ensure that everyone, especially newly assigned personnel who might have to take part, will be able to carry out their duties. When necessary, the plan should be changed based on the lessons learned during the rehearsal. Rehearsals will be documented (date of rehearsal, what was rehearsed, and who participated) and the documentation made available to inspectors and auditors.

b. At locations inside the U.S., the emergency plans will be rehearsed at least semiannually.

c. In locations outside the U.S., the plan will be rehearsed at least quarterly.

d. In high-risk areas, the CAM will review the plan with all account personnel monthly and conduct a rehearsal at least quarterly.

e. Each rehearsal may cover only a portion of the entire plan. However, the CAM will ensure that all aspects of the plan have been rehearsed at least once each year.

9–6. After action requirements

a. Whenever emergency plans including precautionary actions are implemented, the key material CONAUTH will be advised immediately regarding the disposition and status of their key. If any centrally accountable COMSEC material was destroyed, a destruction report will be submitted to the central office of record. If any material was lost or compromised, an incident report must be prepared in accordance with chapter 6. This does not apply to rehearsals or "dry runs" conducted for the purpose of verifying the execution of emergency plans or for training personnel.

b. When the implementation of emergency plans results in the abandonment of COMSEC material, a timely reasonable effort should be made to recover the material. The extent of this effort will be based on the likelihood of success without exposing people to undue danger. Recoverable COMSEC material will be collected and placed under the control of authorized cleared persons until disposition instructions are received from USACSLA.

Appendix A
References

Section I
Required Publications

AR 25–2
Information Assurance (Cited in paras 1–12*o*, 1–14*b*, 2–2*u*, 2–7*c*, 8–9*d*, 8–22*c*, 8–31, and B–10*b*(9).)

AR 25–55
The Department of the Army Freedom of Information Act Program (Cited in paras 1–13, 6–6*d*, 8–57*e*, and B–7.)

AR 190–51
Security of Unclassified Army Property (Sensitive and Nonsensitive) (Cited in paras 1–12*m*, 2–33*i*(4), 3–7*b*, 8–6, 8–8, 8–8*a*, 8–8*c*(2), 8–9*d*, 8–22*c*, 8–23*f*, 8–31*a*, 8–44*a*, and 8–57*a*(5).)

AR 380–5
Department of the Army Information Security Program (Cited in paras 2–13*c*, 2–23*d*, 2–25, 2–33, 2–33*i*(1), 2–33*m*, 2–35, 2–36*a*, 2–38, 2–38*b*(1), 2–38*d*(4)*(b)*, 2–38*f*, 2–38*k*, 3–5g, 3–5h, 6–12*d*(1), 6–13*b*, and B–1.)

AR 380–27
Control of Compromising Emanations (Cited in para 2–23*d*.)

AR 380–67
The Department of the Army Personnel Security Program (Cited in paras 2–8*c*, 6–1*f*, and 7–3*g*.)

AR 710–2
Inventory Management Supply Policy Below the National Level (Cited in paras 1–1, 1–12*g*, 2–13*b*, 2–14*d*, 8–12, 8–13*a*, 8–14*e*, 8–15*b*, 8–16*b*, 8–16*d*, 8–18*a*, 8–18*d*, 8–35*c*(2), 8–35*f*, 8–51*e*, and E–4*i*.)

AR 710–3
Asset and Transaction Reporting System (Cited in paras 1–1, 1–12*g*, 8–5*a*, 8–7*a*(10), 8–12, 8–16, and 8–48*d*(5).)

DA Pam 190–51
Risk Analysis for Army Property (Cited in paras 1–12*m*, 8–7*b*, 8–9*d*, 8–16*f*, 8–22*c*, and 8–23*f*.)

DOD 4500.9–R
Defense Transportation Regulation (Cargo Movement) (Cited in para 2–38*f*.) (Available at http://www.dtic.mil/whs/directives/index.html.)

TB 380–41
Procedures for Safeguarding, Accounting and Supply Control of COMSEC Material (Cited in paras 1–1, 1–14*a*(6), 2–2*t*, 2–3*a*, 2–3*k*, 2–3*p*, 2–13*b*, 2–13*c*, 2–14*a*, 2–17*a*, 2–26*c*, 2–26*h*, 2–26*k*, 2–28*c*, 2–30*b*, 2–33, 2–34*d*, 2–36*a*, 2–37*a*, 2–38, 2–38*d*(4)*(c)*, 2–38*j*, 3–1*b*, 3–1*d*, 3–2*a*, 3–2*c*, 3–3, 3–5*b*, 3–5*h*, 4–3*t*, 4–13, 5–3, 5–3*b*, 5–3*c*, 5–4*d*, 6–6*a*, 6–12, 6–12*d*(3), 6–15, 8–14*b*, 8–16*f*, 8–17*b*, 8–25, 8–26*a*, 8–30, 8–48*d*(4), 8–50*b*, 8–51, 8–55*a*, 8–56, 8–57*c*, 9–1, B–1, C–3*d*, E–4*f*, and E–4*m*.)

Section II
Related Publications
A related publication is a source of additional information. The user does not have to read it to understand this regulation.

AR 11–2
Managers' Internal Control Program

AR 15–6
Procedures for Investigating Officers and Boards of Officers

AR 25–12
Communications Security Equipment Maintenance and Maintenance Training

AR 25–30
The Army Publishing Program

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

AR 190–11
Physical Security of Arms, Ammunitions and Explosives

AR 190–13
The Army Physical Security Program

AR 190–16
Physical Security

AR 380–10
Foreign Disclosure and Contacts with Foreign Representatives

AR 380–49
Industrial Security Program

AR 381–10
U.S. Army Intelligence Activities

AR 381–12
Threat Awareness and Reporting Program

AR 381–14
Technical Counterintelligence (TCI) (C)

AR 381–20
The Army Counterintelligence Program

AR 381–143
Nonstandard Material Policy and Procedures (U)

AR 708–1
Logistics Management Data and Cataloging Procedures for Army Supplies and Equipment

AR 710–1
Centralized Inventory Management of the Army Supply System

AR 725–50
Requisitioning, Receipt, and Issue System

AR 735–5
Policies and Procedures for Property Accountability

AR 735–11–2/DLAI 4140.55/SECNAVINST 4355.18A/AFJMAN 23–215
Reporting of Supply Discrepancies

AR 740–26
Physical Inventory Control

AR 750–1
Army Material Maintenance Policy

CJCSI 3260.01C
Joint Policy Governing Positive Control Material and Devices (This classified directive is not approved for electronic release. Distribution is at the sole discretion of the office of primary responsibility.)

CJCSI 6510.02D
Chairman of the Joint Chiefs of Staff Instruction Communications Security Releases to Foreign Nations (Available at http://www.dtic.mil/cjcs_directives/.)

CJCSI 6510.06B
Crytographic Modernization Plan (Available at http://www.dtic.mil/cjcs_directives/.)

CNSS Instruction No. 4004.1
Destruction and Emergency Protection Procedures for COMSEC and classified Material with amended Annex B (Available at http://www.cnss.gov/.)

CNSS Policy No. 1
National Policy for Safeguarding and Control of COMSEC Materials (Available at http://www.cnss.gov/.)

CNSS Policy No. 3
National Policy on Granting Access to U.S. classified Cryptographic Information (Available at (Available at http://www.cnss.gov/.)

CNSS Policy No. 14
National Policy Governing the Release of INFOSEC Products or Associated INFOSEC Information to Authorized U.S. Activities that are Not a Part of the Federal Government (Available at http://www.cnss.gov/.)

CNSSI Policy No. 4005
Safeguarding Communications Security (COMSEC) Facilities and Material (Available at http://www.cnss.gov/.)

CNSSI Policy No. 4009
National Information Assurance (IA) Glossary (Available at http://www.cnss.gov/.)

CNSSI Policy No. 7000
TEMPEST Countermeasures for Facilities (Available at http://www.cnss.gov/.)

DA Pam 25–30
Consolidated Index of Army Publications and Blank Forms

DA Pam 710–2–1
Using Unit Supply System (Manual Procedures)

DA Pam 710–2–2
Supply Support Activity Supply System: Manual Procedures

DOD 4160.21–M
Defense Material Disposition Manual

DOD 5105.38–M
Security Assistance Management Manual (SAMM)

DOD 5200.1–R
Information Security Program

DOD 5200.2–R
Department of Defense Personnel Security Program

DOD 5220.22–M
National Industrial Security Program Operating Manual

DOD 5220.22–R
Industrial Security Regulation

DODD 5210.48
Polygraph and Credibility Assessment Program

DODD 8500.01E
Information Assurance

DODD 8570.01
Information Assurance (IA) Training, Certification, and Workforce Management

DODI 5205.08
Access to classified Cryptographic Information

DODI 5210.91
Polygraph and Credibility Assessment (PCA) Procedures

DODI 8523.01
Communications Security (COMSEC)

EO 12333
United States intelligence activities

EO 13526
Classified National Security Information

Federal Aviation Administration Advisory Circular 108–3
Screening of Persons Carrying U.S. Classified Material (Available at http://rgl.faa.gov/Regulatory_and_Guidance_Library/rgAdvisoryCircular.nsf/list/AC%20108-3/$FILE/AC108-3.pdf.)

FF–L–2740B
Locks, Combination, Electromechanical (Available at https://portal.navfac.navy.mil/portal/page/portal/navfac/navfac_ww_pp/navfac_nfesc_pp/locks/dodlock_fedspecs.)

FF–P–110J
Padlock, Changeable Combination (Resistant to Opening by Manipulation and Surreptitious Attack) (Available at https://portal.navfac.navy.mil/portal/page/portal/navfac/navfac_ww_pp/navfac_nfesc_pp/locks/dodlock_fedspecs.)

Intelligence Community Standards 705–1
Sensitive Compartmented Information Facilities (Available at http://www.dni.gov/electronic_reading_room/ICD_705_SCIFs.pdf.)

JP 1–02
DOD Dictionary of Military and Associated Terms

MIL–STD 188 Series
Military Communication System Technical Standards (Available at http://dodssp.daps.dla.mil/.)

NAG–16
Field Generation and Over-the-Air Distribution of COMSEC Key in Support of Tactical Operations and Exercises (Available at http://www.iad.nsa.smil.mil/resources/library/nags_section/index.cfm.)

NAG–53
Keying standards for nontactical KG–84A/C and KIV–7HS (high speed), KIV–7HSA, and KIV–7HSB communications security (COMSEC) equipment in DOD nontactical point-to-point applications (Available at http://www.iad.nsa.smil.mil/resources/library/nags_section/index.cfm.)

National Security Directive 42
National Policy for the Security of National Security Telecommunications and Information Systems

NSA/CSS Manual 1–52
Security Classification Guide for Intelligence and Surveillance (Available at http://www.nsa.gov/.)

NSA/CSS Manual 3–16
Control of Communications Security (COMSEC) Material (Available at http://www.nsa.gov/.)

NSTISSI No. 4000
COMSEC Equipment Maintenance and Maintenance Training (Available at http://www.cnss.gov/.)

NSTISSI No. 4001
Controlled Cryptographic Items (Available at http://www.cnss.gov/.)

NSTISSI No. 4003
Reporting and Evaluating COMSEC Incidents (Available at http://www.cnss.gov/.)

NSTISSI No. 4006
Controlling Authorities for COMSEC Material (Available at http://www.cnss.gov/.)

NSTISSI No. 4010
Keying Material Management (Available at http://www.cnss.gov/.)

NSTISSP No. 8
National Policy Governing the Release of INFOSEC Products or Associated INFOSEC Information To Foreign Governments (Available at http://www.cnss.gov/.)

SB 700–20
Army Adopted Items of Materiel and List of Reportable Items

44 USC 3542
Definitions Available at http//www.gpoaccess.gov/uscode.)

RCSGID–131
Cryptosystems Evaluation Report

Section III
Prescribed Forms
This section contains no entries.

Section IV
Referenced Forms
Except where otherwise indicated below, DA Forms are available on the APD Web site (http://www.apd.army.mil) and DD Forms are available on the Office of the Secretary of Defense Web site (http://www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm). SFs are available on the GSA Web site http://www.gsa.gov/portal/forms/type/SF.

DA Form 11–2
Internal Control Evaluation Certification

DA Form 1999
Restricted Area Visitor Register

DA Form 1687
Notice of Delegation of Authority – Receipt for Supplies

DA Form 2028
Recommended Changes to Publications and Blank Forms

DA Form 2653–R
COMSEC Account - Daily Shift Inventory

DD Form 254
Department of Defense Contract Security Classification Specification

DD Form 1435
COMSEC Maintenance Training and Experience Record

DD Form 1907
Shipment Signature and Tally Record

DD Form 2501
Courier Authorization Card

DD Form 2625
Controlled Cryptographic Item (CCI) Briefing

Form DSP–5
Application/License for Permanent Export of Unclassified Defense Articles and or Related Technical Data (Available at http://www.pmddtc.state.gov/DTRADE/.)

Form DSP 73
Application/License for Temporary Export of Unclassified Defense Articles (Available at http://www.pmddtc.state.gov/DTRADE/.)

SD Form 572
Cryptographic Access Certification and Termination (Available at http://www.dtic.mil/whs/directives/infomgt/forms/eforms/sd0572.pdf.)

SF 153
COMSEC Material Report

SF 700
Security Container Information

Appendix B
Classification Guidelines for Communications Security Information

This appendix provides classification guidance for COMSEC information.

B–1. Applicability and implementation

The information contained in this appendix is applicable to all persons who classify, mark, or handle COMSEC information. The information contained in this appendix will be given appropriate dissemination on a need-to-know basis. In instances where more stringent classification guidance exists, (for example, in AR 380–5 or system specific security guidance) that guidance will be used. All classification guidance for contractors is to be via a completed and approved DD Form 254 (see DOD 5220.22–R). Queries concerning COMSEC-related topics or subjects should be directed to Office of the DCS, G–2 (DAMI–CDS). In addition, TB 380–41 provides additional information on classification guidelines.

B–2. Duration

Unless a particular item of COMSEC information will become declassified at a particular time or following a specific event, the guidance prescribed herein has indefinite duration. Information Classified according to this appendix will be marked—Derived from: NSA/CSS Manual 1–52, dated, 8 January 2007, Declassify on: 25 years and in accordance with applicable security classification guides. In those instances where documents are prepared from multiple sources, the declassification date or event that provides the longest period of classification will be used.

B–3. Definitions

The definitions contained in DA Pam 25–30, JP 1–02, and glossary of this AR apply.

B–4. Crypto marked information

The following guidance is provided with respect to the marking crypto:

a. Documents, correspondence, messages, memorandum, publications, reports, and specifications will not be marked crypto unless they contain cryptographic key.

b. In documents that require the crypto caveat, the caveat will appear at the bottom of each page immediately following the classification. The crypto caveat will always be capitalized.

B–5. Foreign release

COMSEC information in any form is not releasable to foreign nationals unless specifically authorized. Requests for

release will be forwarded through command channels to DCS, G–2 (DAMI–CDS). When a determination has been made that there is a risk of unauthorized foreign access to specific classified COMSEC material or when a specific prior determination has been made that the material will not be released, it will be marked NOT RELEASABLE TO FOREIGN NATIONALS (NOFORN). Regardless of the presence or absence of the NOFORN marking, no COMSEC material or information may be released to a foreign nation, foreign national, or an international organization without the express written authorization of the DCS, G–2 (DAMI–CDS).

B–6. Communications security equipment and related documentation

The classification of all COMSEC equipment used to protect or authenticate classified national security information, other sensitive but unclassified Government or Government-derived information, or transmission security processes is determined by NSA. Guidance for the classification and marking of such equipment and the documentation associated with their development, production, maintenance, and use are set forth below.

a. Documentation pertaining to cryptographic logic. In development contracts, documentation pertaining to cryptographic logic, including crypto algorithms and any associated software coding, will normally be classified secret and declassified only upon the determination of the originating agency.

b. Production of unclassified communications security equipment. Production of unclassified COMSEC equipment is normally done in uncleared contractor facilities. However in production contracts, documentation pertaining to the cryptographic logic of such equipment will be classified at least confidential and will be declassified only upon the originating agency's determination.

c. Production of classified communications security equipment. Production of classified COMSEC equipment must be done in cleared facilities. In production contracts, documents pertaining to the cryptographic logic of such equipment will be classified at least at the level of the associated equipment and will be declassified only upon the originating agency's determination.

d. Full maintenance manuals. COMSEC software and other technical documentation that provide detailed schematics or descriptions of the cryptographic circuits of specific cryptosystems will be classified at least confidential and will be declassified only upon the originating agency's determination.

e. Items impossible to physically mark. Because of the size or configuration, it may be impossible to physically mark certain COMSEC items with the required classification authority and declassification notice. In such cases, these notices will be included on the associated documentation or packaging and tagged on the item itself until installed.

B–7. Application of the marking for official use only

The marking FOUO is to be used only for information that may be withheld from the public for one or more reasons cited in AR 25–55. The marking "FOUO" will be applied to unclassified COMSEC information (according to AR 25–55) when the preparing organization determines that such information qualifies for the FOUO marking under the Freedom of Information Act. The acronym FOUO is to be used for individual paragraphs when required and for electronic communications. The marking FOUO should be considered for the following types of unclassified information:

a. Narrative technical information on the characteristics of COMSEC equipment.

b. Indications of new COMSEC developments.

c. Any COMSEC planning, programming, and budgeting information.

d. Specifications and purchase descriptions pertaining to COMSEC equipment or the support of unique COMSEC requirements.

e. Publications on ancillary equipment developed exclusively for use with COMSEC equipment.

f. Handling instructions and doctrinal information relating to COMSEC material.

g. Manual cryptosystems produced exclusively for sample and unclassified training purposes.

h. Unclassified COMSEC material reports (SF 153).

B–8. Compilation of unclassified communications security information that may warrant classification

When unclassified COMSEC information is assembled for publication, good judgment must be exercised by the preparing organization in deciding whether such information in the aggregate needs classification before publication. The classification authority should carefully weigh the value of COMSEC information to hostile intelligence organizations and consider whether access to the information would assist these organizations in deploying their collection and analytical resources in exploitation efforts, especially when the information contains details about new systems employing COMSEC equipment. Following are examples of compilations of unclassified information that may require a minimum classification of confidential.

a. Detailed planning and implementation information on COMSEC equipment to be deployed. Additionally, planning or operational information that could be used by foreign intelligence activities for targeting.

b. Information on cryptosystems, equipment, and components in development or to be fielded together, with amplifying details such as how, when, where, and why the equipment is to be deployed and used.

c. Complete parts list for COMSEC equipment.

d. A complete or substantially complete listing of unclassified short and long titles of equipment in the department or agency COMSEC inventory and their supporting documents.

e. Compilations of narrative technical information describing the characteristics and functions of classified COMSEC equipment.

f. Total COMSEC program and budget information for individual departments and agencies.

B–9. Key classification

Normally key will be assigned a classification equal to the highest classification of the information to be encrypted.

B–10. Communications security classifications

a. General.

(1) Operational, exercise, and training key being used where information is transmitted using telecommunications. Classify based on content of information protected. They are marked crypto.

(2) Training key being used in a classroom or other situations where information is not transmitted. Classify based on content of the information protected. Usually the key is marked to resemble operational key with the note FOR TRAINING ONLY.

(3) Test key for online testing of equipment. Classify based on net circuitry or intended level of information and equipment parameters protected. It is marked crypto.

(4) Maintenance key for offline or in-shop use. Classify based on intended level of information and equipment parameters being protected.

(5) Sample key for demonstration use. Classify based on content. Normally it is marked to resemble operational key.

(6) Cryptographic ignition key (unclassified).

b. Crypto equipment characteristics.

(1) Information that reveals that equipment encrypts, decrypts, or conforms to Military Standard (MIL–STD) 188 Series or the fact that equipment has antijam or low probability-of-intercept capability is unclassified.

(2) The fact that a COMSEC equipment item has an antitheft or antispoof capability is confidential.

(3) Identification of a particular COMSEC equipment item with a particular system is unclassified FOUO.

(4) Interface control documents or specifications that include descriptive amplifying information regarding COMSEC functions, rules or motion, internal activities, and security techniques are classified at the level of the equipment cryptologic.

(5) Information indicating that a specific COMSEC equipment item employs a cover named cryptographic logic is unclassified.

(6) Information concerning COMSEC equipment if it reveals or can be associated with any of the following types of information about an equipment item:

(a) Specific cryptologic details and parameters information is secret.

(b) Specific antitamper and antitapping design details and parameters information is secret NOFORN.

(c) Reasons for certain design features information is secret NOFORN. It may bear higher classification than the details of the design.

(7) Information concerning test equipment (for example, factory, field, or depot test equipment) reflecting any of the information covered in paragraph B–10*b* is classified secret.

(8) Magnetic media (for example, core memory disks, drums, and tapes) that have held key designated crypto must retain the highest classification of any information previously recorded on them. They cannot be declassified.

(9) Magnetic media that have never held key designated crypto may be declassified using the procedures in AR 25–2.

(10) Classify information as secret, including photo masters, drawings, etched boards, and diagnostic test routines of classified COMSEC equipment and components, such as printed circuit boards, modules, if the information reveals the same as may be obtained from an examination of the complete component.

(11) The fact that a randomizer is used in a specific COMSEC equipment or crypto algorithm is unclassified and/or FOUO.

(12) The randomizer itself and documentation that reveals the complete design are confidential.

c. Computer cryptographic system characteristics.

(1) The fact that a computer performs a COMSEC function, such as encryption, decryption, authentication, or control of a piece of COMSEC hardware is unclassified.

(2) Classification of the details of a specific computer crypto algorithm interface program will be determined by the NSA on a case-by-case basis.

(3) Specific details and parameters of computer crypto algorithms or information that reveals the exact length of key is classified secret.

(4) Computer crypto algorithm diagnostic checks are classified a minimum of confidential.

(5) The classification of access control techniques, such as passwords and authentication systems, is determined by the DCS, G–2 (DAMI–CDS) on a case-by-case basis.

d. Usage.

(1) Implementation or supersession dates of—

(a) A single item of classified key marked crypto are classified confidential unless specified otherwise in an operating instruction or other document.

(b) A general or instructional COMSEC publication is unclassified and/or FOUO.

(2) Circuit status information is classified as follows:

(a) Information pertaining to a single sealed authenticator for use in command and control is classified secret.

(b) Circuit status charts that reveal cryptoperiods of classified key is unclassified and/or FOUO unless specified otherwise in an operating instruction or other document.

(c) Filled in operational certificates indicating use of classified key are confidential unless specified otherwise in an operating instruction or other document.

(3) The identification of COMSEC material suspected of being compromised is classified confidential, unless it pertains to 2 person control material, in which case it is classified secret.

(4) Cryptoperiods-related information revealing the length of a cryptoperiod of classified COMSEC key is normally unclassified and/or FOUO. However, NSA may classify nonstandard or special cryptoperiods.

(5) Information that reveals only the specific application of an equipment item (for example, to secure the communications of a specific network or command) is unclassified.

e. Weapons and space systems.

(1) The fact that NSA or one of the Service cryptologic elements is associated with a space or weapons system, that a space or weapons system has a cryptographic capability, or the identification of specific COMSEC equipment by short title with a specific space or weapons system is unclassified and/or FOUO. The mere existence of certain space and weapons systems is classified.

(2) Details of amplification of the cryptographic capabilities, characteristics, or limitations of a specific space system are classified secret NOFORN. Depending upon the details or amplification, the classification may be top secret NOFORN.

(3) The exact location of a satellite or weapons system containing classified COMSEC hardware following reentry into the earth's atmosphere is secret NOFORN.

(4) Details or amplification of the cryptographic capabilities, characteristics, or limitations of a weapon system are confidential NOFORN.

(5) Information revealing the extent of support furnished by NSA for a specific space system is secret NOFORN at a minimum and, depending upon the program involved, may be top secret.

(6) Information revealing the extent of support furnished by NSA for a specific weapons system is secret unless specifically downgraded.

(7) Information or evaluation revealing the vulnerability of a weapons system's COMSEC subsystem and associated storage media is top secret NOFORN.

(8) Launch evaluations of weapons systems and COMSEC subsystems that reveal weaknesses or threats that may be applicable to other weapons systems are top secret NOFORN.

(9) Evaluations that reveal the vulnerability of a space COMSEC system to cryptanalysis are top secret NOFORN.

f. Abandonment and recovery of communications security material.

(1) The location of a recovery area when release of the location is essential to save or protect human life is unclassified and/or FOUO. The location is releasable to any person or nation by any communications means that will expedite the search and rescue efforts. The fact that COMSEC material may be recoverable should not be mentioned in the communication.

(2) The fact that key or keyed COMSEC equipment of a particular site or element may have been compromised is confidential. It may be transmitted in the clear if essential to emergency supersession actions to minimize damage from compromise and if no secure communications means is available.

(3) The location of recovery or abandonment area when key or keyed COMSEC equipment is involved is classified at the same level as the key involved when preservation of life is not an issue.

(4) The location of recovery or abandonment area for classified COMSEC equipment or logic is secret when the preservation of life is not an issue.

(5) The location of recovery or abandonment area of unkeyed CCI and confidential COMSEC aids is confidential when preservation of life is not an issue.

g. Security fault analysis, crypto analysis, cryptokey extraction, tampering, or bugging.

(1) The classification of the terms security fault analysis, crypto analysis, failure modes and logic effects, key extraction analysis, and tampering or bugging analysis, as well as, their definitions, is unclassified.

(2) The statement that equipment may contain security fault deficiencies without mentioning specific deficiencies or effects is confidential.

(3) Statements and details about specific unremedied weaknesses of COMSEC equipment or functions within a system, including specific vulnerabilities to crypto analysis, TEMPEST, exploitation, tampering, key extraction, and security fault analysis are top secret NOFORN.

(4) A statement about the types of security fault deficiencies and their effects is secret NOFORN.

(5) The statement, without giving details, that particular equipment has a cryptanalytic weakness is secret NOFORN.

(6) The statement, without giving details, that the security life of a particular equipment (including CCI) extends to the year (XXXX) is secret NOFORN.

(7) A statement about the types of key extraction or tampering or bugging attacks secret NOFORN.

(8) The statement that specific equipment contains no security fault deficiencies or that specific equipment is not vulnerable to key extraction or tampering and bugging attacks is unclassified.

(9) The statement, without details, that specific equipment contains security fault deficiencies or that specific equipment is vulnerable to key extraction or tampering and bugging attacks is secret NOFORN.

(10) The description of types of attacks related to key extraction or tampering and bugging without mentioning specific equipment is secret NOFORN.

(11) The statement giving details that specific equipment (in its preproduction phases of development) contains security fault deficiencies is secret NOFORN.

(12) The statement giving details that specific equipment contains security fault deficiencies, information revealing specific components or circuits within specific equipment designed to protect against security fault deficiencies, or security fault analysis type information that reveals specific information about crypto analytic attacks on equipment is top secret NOFORN.

h. Communications security records and reports.

(1) Production records or forms for classified key when these indicate the material by short title, copies per edition, and quantity produced, but not the effective date, is unclassified and/or FOUO. Compilations of these records or forms are also unclassified.

(2) Lists of COMSEC material that are not crypto holdings (inventories) are unclassified.

(3) The identification of specific COMSEC equipment, component, system, or key (to include identification by short title), or listing of such, with or without association with the identification of the specific location or facility to which it is being deployed, or at which it will be operationally used is unclassified.

(4) Inventory reports of COMSEC material that list only unclassified material, and all negative inventory reports are unclassified.

(5) Individual accounting reports (for example, transfer, possession, and destruction) and individual accounting reports involving DOD contractors are normally unclassified and/or FOUO, unless the reports contain classified addresses or classified information in the remarks block. Reports relating to material controlled by CJCSI 3260.01C will be classified confidential. If the effective material is designated, the classification will be secret.

(6) Administrative or managerial reports containing information relative to total inventory of specified classified COMSEC equipment held by a department or agency is normally confidential. Depending on the holdings, it may be secret or unclassified and/or FOUO.

(7) COMSEC audit reports and command COMSEC inspection reports that show no discrepancies with the crypto holdings or that describe poor procedures or conditions that cannot be used to breach facility security are unclassified and/or FOUO.

(8) Reports that contain information that could be used to mount a physical, cryptographic, TEMPEST, communications intelligence, or human intelligence attack against a facility or its personnel is classified a minimum of confidential.

(9) COMSEC incident reports, audit reports, and other accounting reports will be classified according to content. Unclassified reports will be marked FOUO.

B–11. Classification guide for controlled cryptographic item Information

a. Association of NSA with development of CCI will be unclassified and/or FOUO.

b. Association of a contractor with the production or research and development of a specific CCI is unclassified and/or FOUO.

c. Identification of a specific algorithm used in a particular CCI is confidential.

d. Description or purpose of the antitamper (quadrant) features associated with CCI is confidential.

e. Specific antitamper and antitapping details and parameters of a CCI is secret NOFORN.

f. The fact that a particular CCI has an antidepth or antispoof capability is confidential.

g. Identification of a particular CCI with the CE or weapons system it secures is unclassified and/or FOUO.

h. Detailed description and/or documentation and associated cryptographic engineering drawings and logic descriptions for a CCI is confidential.

i. Hardware or firmware embodiment of a classified algorithm associated with CCI end items or CCI (crypto) components is confidential.

j. Description or discussion of equipment designated CCI while in research and development is confidential.
k. Narrative technical information on the characteristics of CCI is unclassified and/or FOUO.
l. COMSEC planning, programming, and budget information is unclassified and/or FOUO.
m. Handling instructions and doctrinal information relating to CCI is unclassified and/or FOUO.
n. All COMSEC reports not otherwise classified is unclassified and/or FOUO.

Appendix C
Physical Security Standards

C–1. General
This appendix provides the general construction standards and special controls unique to fixed COMSEC facilities in a nontactical environment other than GSA-approved security containers. Work areas not considered COMSEC facilities that contain COMSEC equipment (for example, KIV–7, STEs, and DTDs), when in their unclassified CCI state (CIK removed and secured separately), must be protected in a manner that affords protection at least equal to what is normally provided to other high value or sensitive material and ensures that access and accounting integrity is maintained.

C–2. Vaults
Vaults used as storage facilities for COMSEC keying material must be constructed in accordance with the following standards:

a. Reinforced concrete construction. Walls, floors, and ceilings will be a minimum thickness of 8 inches of reinforced concrete. The concrete mixture will have a comprehensive strength rating of at least 2,500 pounds per square inch. Reinforcing will be accomplished with steel reinforcing rods, a minimum of 5/8 inch in diameter, positioned centralized in the concrete pour and spaced horizontally and vertically 6 inches on center; rods will be tied or welded at the intersections. The reinforcing is to be anchored into the ceiling and floor to a minimum depth of half the thickness of the adjoining member. Walls consisting of cement block do not meet the standards for vault construction.

b. Steel-lined construction. Where unique structural circumstances do not permit construction of a concrete vault, construction will be of steel alloy-type of 1/4 inch thickness, having characteristics of high yield and tensile strength. The metal plates are to be continuously welded to load-bearing steel members of a thickness equal to that of the plates. If the load-bearing steel members are being placed in a continuous floor and ceiling of reinforced concrete, they must be firmly affixed to a depth of half the thickness of the floor and ceiling. If the floor or ceiling construction is less than 6 inches of reinforced concrete, a steel liner is to be constructed the same as the walls to form the floor and ceiling of the vault. Seams where the steel plates meet horizontally and vertically are to be continuously welded together.

c. Vault door. All vaults will be equipped with a GSA-approved Class 5 or Class 8 vault door. Within the U.S., a Class 6 vault door is acceptable. Normally within the U.S. a vault will have only one door that serves as both entrance and exit from the facility in order to reduce costs.

C–3. Secure rooms
All secure rooms used for COMSEC facilities must be constructed of material that will deter and detect covert penetration. Facilities must be constructed so that classified information cannot be overheard through walls, doors, windows, ceilings, air vents, and ducts when secure areas border on unsecure areas. The following requirements are not applicable to continuously attended bulk encryption facilities. Alternate construction standards may be approved when supplemental security systems (for example, intrusion alarms, armed guards, and video cameras) are used. Requests for approval of alternate construction standards will be forwarded through command channels to the ACOM, ASCC, or DRU command security office for consideration to the DCS, G–2 (DAMI–CDS), with a copy furnished to USACSLA (AMSEL–LCA–SAS).

a. Walls, floors, and ceilings. Outer walls, floors, and ceilings of the building must be permanently constructed and attached to each other. All construction must be done in such a manner as to provide visual evidence of unauthorized penetration. All openings will provide sufficient sound attenuation to preclude inadvertent disclosure of conversations. Intelligence Community Standards 705–1 is available at http://www.dni.gov/electronic_reading_room/ICD_705_SCIFs.pdf and these standards will be referred to as the national standard for acoustical control and sound masking techniques.

b. Main entrance door. Only one door should be used for regular entrance to the facility. The door must be strong enough to resist forceful entry. In order of preference, examples of acceptable doors are GSA-approved vault doors; standard 1 3/4 inch, internally reinforced, hollow metal industrial doors; and metal-clad or solid hardwood doors at least 1 3/4 inch thick. The door frame must be securely attached to the facility and fitted with a heavy-duty, high-security strike plate and hinges installed with screws long enough to resist removal by prying. The door must be

installed to resist the removal of the hinge pins by locating the hinge pins inside the facility or by set screwing or welding the pins in place.

c. Other doors. Other doors may exist for emergency exit and for moving bulky items. These doors must meet the construction criteria of the main entrance door and must be designed so that they can be opened only from inside the facility. Approved panic hardware, intrusion detection, and locking devices (lock bars, dead bolts, knobs, or handles) may be placed only on the interior surfaces of other doors to the facility. Emergency escape mechanisms that bypass the built-in combination lock should be double-latched. All doors must remain closed during facility operations and must be opened only for passage of authorized personnel or material.

d. Security locking devices. The main entrance door to facilities that are not continuously attended must be equipped with a GSA-approved electro-mechanical lock meeting Federal Specification (FF–L–2740A) and amendment 1. A built-in lock is not required for facilities continuously attended; however, the door must be able to accommodate the above lock and a dead bolt should it ever become necessary to lock the facility from the outside. An electronically actuated lock (that is, cipher lock or keyless push button lock) may be used on the entrance door to facilitate the admittance of authorized personnel when the facility is attended. However, these locks do not afford the required degree of protection and may not be used to secure the facility when it is not attended. Facility occupants must maintain positive control of the entrance at all times while attended regardless of the locking mechanism. See TB 380–41 for specifics on approved security locking and access control devices.

e. Windows. COMSEC facilities should not contain windows. Where windows exist that might reasonably afford visual surveillance of personnel, documents, materials, or activities within the facility, the window will be made opaque or equipped with blinds, drapes, or other coverings to preclude such visual surveillance. Windows that are less than 18 feet above the ground (measured from the bottom of the window) or are easily accessible by means of objects directly beneath the window will be constructed from or covered with materials that will provide protection from forced entry. Facilities located within fenced and guarded U.S. Government compounds or equivalent may eliminate this requirement if the windows are made inoperable by permanently sealing them.

f. Other openings. Air vents, ducts, or any similar openings that breach the walls, floor, or ceiling of the facility must be appropriately secured to prevent penetration. Openings less than 96 inches must have approved baffles installed to prevent an audio or acoustical hazard. If the opening exceeds 96 inches, acoustical baffles must be supplemented by either hardened steel bars or an approved intrusion detection system.

C–4. Nonstandard facilities

When a commander or other responsible official is required to establish and operate a facility with keyed COMSEC equipment to process classified National Defense Information up to the secret level, and a room or building meeting the standards of C–2 or C–3 are not available, a permanently constructed facility that provides a reasonable level of security and control may be utilized, when all of the following measures are adhered to:

a. The room or structure must be completely enclosed with all sides, floor, and ceiling permanently connected to one another. All entrances and other openings must be secured, with the doors using a high security padlock when unoccupied, to the extent that any attempt at forced or surreptitious entry can be detected.

b. A formal risk analysis and/or assessment must be completed and a detailed narrative prepared in memorandum format presenting all pertinent facts and circumstances submitted through the requesting official's chain of command to the 1st general officer requesting approval for the facility.

c. With due consideration of the risks involved, local security conditions, and sensitivity of the COMSEC equipment and the information it protects, responsible officials must make a formal determination as to the need for protecting the COMSEC equipment with locking bars or specially designed security containers, and supplemental protection of the facility itself with guards, roving patrols, and alarms. All such protective measures must be detailed in the request for approval.

d. Nonstandard facilities will not be used at the top secret level unless approved by the ACOM, ASCC, or DRU commander. A copy of such approvals for top secret facilities will be provided to the DCS, G–2 (DAMI–CDS) for review.

Appendix D
Cryptographic Access Briefing

D–1. Indoctrination briefing

The following briefing must be used verbatim to indoctrinate individuals for cryptographic access:

a. You have been selected to perform duties that will require access to classified cryptographic information. It is essential that you be made aware of certain facts relevant to the protection of this information before access is granted. You must know the reason why special safeguards are required to protect classified cryptographic information. You must understand the directives that require these safeguards and the penalties you will incur for the unauthorized disclosure and/or retention or negligent handling of classified cryptographic information under the criminal laws of the

United States. Failure to properly safeguard this information could cause exceptionally grave damage or irreparable injury to the national security of the United States or could be used to advantage by a foreign nation.

b. Classified cryptographic information is especially sensitive because it is used to protect other classified information. Any particular piece of cryptographic key and any specific cryptographic technique may be used to protect a large quantity of classified information during transmission. If the integrity of a cryptographic system is breached at any point, all information protected by the system may be compromised. The safeguards placed on classified cryptographic information are a necessary component of Government programs to ensure that our Nation's vital secrets are not compromised.

c. Because access to classified cryptographic information is granted on a strict need-to-know basis, you will be given access to only that cryptographic information necessary in the performance of your duties. You are required to become familiar with AR 380–40 as well as those publications referenced therein.

d. Especially important to the protection of classified cryptographic information is the timely reporting of any known or suspected compromise of this information to (insert the CAM or the appropriate security office). If a cryptographic system is compromised, but the compromise is not reported, the continued use of the system can result in the loss of all information protected by it. If the compromise is reported, steps can be taken to lessen an adversary's advantage gained through the compromise of the information.

e. As a condition of access to classified cryptographic information, you must acknowledge that you may be subject to a counterintelligence scope polygraph examination. This examination will be administered in accordance with DODD 5210.48 and applicable law. The relevant questions in this polygraph examination concern espionage, sabotage, unauthorized disclosure of classified information, and unreported foreign contacts. If at this time you do not wish to sign such an acknowledgment as a part of executing a cryptographic access certification, this briefing will be terminated and the briefing administrator will so annotate the cryptographic access certificate. Such refusal will not be cause for adverse action, but will result in your being denied access to classified cryptographic information.

f. Intelligence services of some foreign governments prize the acquisition of classified cryptographic information. They will go to extreme lengths to compromise U.S. citizens and force them to divulge cryptographic techniques and materials that protect the Nation's secrets around the world. Any personal or financial relationship with a foreign government's representative could make you vulnerable to attempts at coercion to divulge classified cryptographic information. Learn to recognize those attempts so that you may successfully counter them. The best personal policy is to avoid discussions that reveal your knowledge of, or access to, classified cryptographic information and thus avoid highlighting yourself to those who would seek the information you possess. Any attempt, either through friendship or coercion, to solicit your knowledge regarding classified cryptographic information must be reported immediately to (insert appropriate security office).

g. In view of the risks noted above, unofficial foreign travel to foreign countries may require the prior approval of (insert appropriate security office). It is essential that you contact (insert appropriate security office) before such unofficial travel.

h. Finally, should you willfully or negligently disclose to any unauthorized persons any of the classified cryptographic information to which you will have access, you may be subject to administrative and civil sanctions, including adverse personnel actions, as well as criminal sanctions under the UCMJ and or Federal law, as appropriate.

D–2. Cryptographic access certification and termination briefing

SD Form 572, section I must be executed before an individual may be granted access to U.S. classified cryptographic information. Section II will be executed when the individual no longer requires such access. Until cryptographic access is terminated and section II is completed, the cryptographic access granting official will maintain the certificate in a legal file system that will permit expeditious retrieval.

a. Individuals will read and sign an official command memorandum containing the briefing (verbatim) in paragraph D–1. In addition they will read and sign section I or section II, as appropriate, of the SD Form 572.

b. SD Form 572 is available at http://www.dtic.mil/whs/directives/infomgt/forms/sdforms.htm.

Appendix E
Internal Control Evaluation

E–1. Function

The function covered by this evaluation is safeguarding and controlling COMSEC material.

E–2. Purpose

The purpose of this evaluation is to assist commanders of units with COMSEC accounts in evaluating key internal controls as mandated by AR 11–2. It is not intended to cover all management control elements.

E–3. Instructions

Answers must be based on the actual testing of key internal controls such as document analysis, direct observation, interviewing, sampling, and simulation. Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation. These internal controls must be evaluated at least once every 5 years. Certification that an evaluation has been conducted must be accomplished on DA Form 11–2 (Internal Control Evaluation Certification).

E–4. Test questions

Examples of questions are as follows:

a. Are key internal controls identified in the governing AR? (Applies to DCS, G–2 only.)

b. Is a CAM appointed for each unit having a COMSEC account as required by this publication?

c. Is the CAM a graduate of the COMSEC Account Manager Course?

d. Is the CAM a graduate of the LMCS?

e. Are required publications, as shown in appendix A, available to COMSEC personnel? Publications do not have to be maintained in the COMSEC account.

f. Is CMCS accountable material being accounted for in compliance with the policy in this publication and the procedures in TB 380–41?

g. Are USACSLA COMSEC audits and inspections being conducted every 24 months?

h. Are command COMSEC inspections being conducted a minimum of once every 24 months?

i. Are all CCI end items of equipment accounted for by serial number on the supporting property account in accordance with AR 710–2?

j. Is TPI used for top secret key operations in accordance with this publication?

k. Are exceptions to TPI approved by DCS, G–2?

l. Do other assigned duties of the CAM permit sufficient time to adequately discharge COMSEC duties?

m. Is the CONAUTH performing those functions required by this publication and TB 380–41?

n. Is the CAM complying with Army COMSEC incident reporting procedures?

o. Does the unit have COMSEC basic emergency plans that address procedures to be used during natural disasters and hostile actions?

p. Are emergency plans rehearsed and the rehearsals documented, as required by this publication?

q. Are unit COMSEC emergency plans compatible with higher command, installation, or activity plans?

r. Is there a CFA on file as required by this publication?

s. Have discrepancies noted in the most recent COMSEC audit and inspection or command COMSEC inspection been corrected?

t. Are records created and managed in accordance with the Army recordkeeping policy?

E–5. Supersession

This evaluation replaces the internal control review checklist previously published in AR 380–40, 30 June 2000.

E–6. Comments

Help make this a better tool for evaluating internal controls. Submit comments to Headquarters, Department of the Army, Deputy Chief of Staff, G–2 (DAMI–CDS), 1000 Army Pentagon, Washington, DC 20310–1000.

Glossary

Section I
Abbreviations

ACOM
Army command

ALC
accounting legend code

AMC
U.S. Army Materiel Command

AMDF
Army master data file

ARNG
Army National Guard

ASCC
Army service component command

CAM
communications security account manager

CARP
communications security account registration packet

CAW
Certification Authority Workstation

CCEP
Commercial Communications Security Evaluation Program

CCI
controlled cryptographic item

CCISP
Controlled Cryptographic Item Serialization Program

CE
communications-electronics

CFA
communications security facility approval

CFAR
communications security facility approval request

CG
Commanding General

CI
counterintelligence

CIIC
controlled inventory item code

CIK
cryptographic ignition key

CIMA
Communications Security Incident Monitoring Activity

CIO/G–6
Chief Information Officer/G–6

CJCSI
Chairman of the Joint Chiefs of Staff Instruction

CLSF
communications security logistic support facility

CMCS
COMSEC Material Control System

CNSS
Committee on National Security Systems

COMSEC
communications security

CONAUTH
controlling authority

COOP
continuity of operations plan

COR
contracting officer's representative

CSP
counterintelligence scope polygraph

CSS
central security service

DA
Department of the Army

DACAP
Department of the Army Cryptographic Access Program

DCS, G–2
Deputy Chief of Staff, G–2

DCS, G–4
Deputy Chief of Staff, G–4

DOD
Department of Defense

DODAAC
Department of Defense Activity Address Code

DRMO
Defense Reutilization and Marketing Office

DRU
direct reporting unit

DSN
defense switched network

DTD
data transfer device

ECU
end cryptographic unit

EKMS
Electronic Key Management System

FOUO
for official use only

GFE
government furnished equipment

GSA
Government Services Administration

HQDA
Headquarters, Department of the Army

HRH
hand receipt holder

IA
information assurance

INFOSEC
information security

INSCOM
U.S. Army Intelligence and Security Command

KEK
key encryption key

KMI
key management infrastructure

KP
key processor

LCMS
Local Communications Security Management Software

LMD
local management device

MIL–STD
Military Standard

MTOE
modified table of organization and equipment

NAG
National Advisory Group

NOFORN
not releasable to foreign nationals

NSA
National Security Agency

NSTISSI
National Security Telecommunications and Information Systems Security Instructions

PBO
property book officer

PCA
Polygraph and Credibility Assessment

PIN
personal identification number

PKI
Public Key Infrastructure

ROTC
Reserve Officers' Training Corps

SD
Secretary of Defense form

SF
standard form

SKL
simple key loader

SOP
standard operating procedure

STE
secure terminal equipment

TB
technical bulletin

TDA
table of distribution and allowances

TPI
two-person integrity

TRADOC
U.S. Army Training and Doctrine Command

TYAD
Tobyhanna Army Depot

UCMJ
Uniform Code of Military Justice

USACSLA
U.S. Army Communications Security Logistics Activity

USPS
U.S. Postal Service

Section II
Terms

Acceptance at destination
U.S. Government official acceptance and assumption of title to property or services at the specified delivery point. This term corresponds generally to the commercial term "FOB destination".

Access
The ability, capability, capacity, and opportunity to obtain detailed knowledge of classified or sensitive information, equipment, or other materials; or the ability and opportunity to have unrestricted or unsupervised use, handling, inspection, or physical control thereof. The particular requirements for authorized access to different categories of COMSEC materials vary. The handling, external viewing of, and physical proximity to CCI by persons not authorized access by under controlled security condition, does not constitute access.

Access control
Measures taken to limit access to the resources of an information system or automated database to authorized users, programs, processes, or other systems.

Accountability
The obligation of an individual to keep official vouchers and other formal accounting records, documents, or funds as prescribed, such as identification data, gains, losses, dues-in, dues-out, and balances on hand or in use in order to establish an audit trail and official record of legitimate ownership.

Accountable officer
A person officially appointed in writing to maintain a formal set of accounting records of property or funds. This person may or may not have physical possession of the property or funds for which he or she maintains accountability.

Active zeroization
This is done by overwriting memory locations before removing all power.

Administrative incident
Administrative incidents are infractions of established COMSEC policies and procedures that are not as serious as those cited as reportable COMSEC incidents in this regulation, but are considered actions that jeopardize the integrity of COMSEC material. Administrative incidents are insecure practices dangerous to security and violations of procedures that require corrective action to ensure the violation does not recur.

Advance shipment notification
The obligation of an individual responsible for shipping CCI to provide prior notification of its impending arrival to the consignee.

Audit trail
Records and documentation supporting debit and credit entries on accounting records from the time property is brought into the Army inventory until final disposition and the property is dropped from accountability.

Authorized activities
Those activities or locations that have a legitimate need, as determined by a U.S. Government department or agency, to protect information that requires processing by national security systems and are, therefore, authorized to have CCIs.

Causative research and/or reconciliation
An investigation of variances in transactions, balances on hand, and administrative management information, as reflected on formal accounting records. The investigation consists of a complete detailed review of all transactions and supporting documents since the last inventory or last reconciliation between custodial and inventory control point accountable records. The purpose of causative research and reconciliation is to assign a cause to a variance so that corrective action can be taken.

Central controlled cryptographic item authority
The element or activity, as designated by the head of a U.S. Government department or agency, charged with

maintaining oversight and management responsibility for all CCI charged to that department or agency (also see COMSEC service authority).

Central office of record
Office of federal department or agency that keeps records of accountable communications security material held by elements subject to its oversight.

Cognizant security authority
That entity designated by the heads of a U.S. Government department or agency charged with responsibility for all physical, technical personnel, and information security matters affecting that department or agency.

Combined facility
A property consisting of a structure, building, or a fixed or mobile shelter or platform that is occupied and operated by U.S. personnel in conjunction with personnel from one of more allied nations.

Combined operations
An operation conducted by U.S. personnel in conjunction with personnel from one or more allied nations. These personnel must act together to accomplish a specific mission.

Command responsibility
The obligation of a commander (or civilian equivalent) to ensure that all Government property and materiel within his or her command is properly safeguarded, used, and cared for and that proper custody and safekeeping of Government property are provided. Command responsibility is inherent with the assumption of command and cannot be delegated. It is evidenced by assignment to a command position at any level and includes the following:

a. Ensuring the security of all property of the command whether in use or in storage.

b. Observing and inspecting subordinates to ensure their activities contribute to the proper custody, care, use, and safekeeping of all property within the command.

c. Enforcing all security, safety, and accounting requirements.

d. Taking administrative or disciplinary measures when necessary to enforce property management policies.

Commercial Communications Security Endorsement Program
A Government program developed to establish a relationship between the NSA and U.S. industry, in which NSA provides the COMSEC expertise (that is, standards, algorithms, evaluations, and guidance), and industry provides design, development, and production capabilities to produce a Type 1 or Type 2 cryptographic device to secure telecommunications, information handling, and computer systems. Such products developed under the CCEP may include modules, printed circuit boards, microcircuits, subsystems, equipment end items, complete systems, or ancillary devices. Commercial items developed under the CCEP are designated CCI.

Communications security
Measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material.

Compatible key
Keying material of a specific short title that can be obtained in both physical form (to be used in the traditional system) and electronic form (to be used with the Army Key Management System) to enable the hard copy key holders to communicate with the electronic key holders.

Compromise
The disclosure of information or data to unauthorized persons or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object or materiel may have occurred.

Communications security account
Administrative entity identified by an account number used to maintain accountability, custody, and control of COMSEC material. Army COMSEC accounts are established when the Army COMSEC Central Office of Record, after receiving notification of COMSEC facility approval from USACSLA, issues a COMSEC account number.

Communications security compromise
Occurs when the COMSEC material is irretrievably lost or when available information clearly proves that the material was made available to an unauthorized person.

Communications security equipment
Equipment designated to provide security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor and, subsequently, by reconverting such information to its original form for authorized recipients. Equipment designed specifically to aid in or as an essential element of the conversion process.

Note. COMSEC equipment includes crypto equipment, crypto ancillary equipment, crypto production equipment, and authentication equipment. Much of today's COMSEC equipment is designated CCI.

Communications security facility
Authorized and approved space used for generating, storing, repairing, or using COMSEC material.

Communications security incident
Occurrence that potentially jeopardizes the security of COMSEC materiel or the secure electrical transmission of national security information.

Communications security incident monitoring activity
The office within a department or agency that maintains a record of COMSEC incidents caused by elements of that department or agency and ensures that all actions required of those elements are completed.

Communications security insecurity
A COMSEC incident which has been investigated, evaluated, and determined to jeopardize the security of COMSEC materiel or the secure transmission of classified or sensitive information.

Communications security material
Item designed to secure or authenticate information. COMSEC material includes, but is not limited to: keys, products, modules, equipment, devices, documents, hardware, firmware, or software that embodies or describes cryptographic logic and other items that perform COMSEC functions.

Communications Security Material Control System
Logistics and accounting system through which COMSEC material marked "crypto" is distributed, controlled, and safeguarded. Included are COMSEC central offices of record, cryptologistic depots, and COMSEC accounts. COMSEC material other than key may be handled though the CMCS.

Communications security service authority
The COMSEC service authority is the department or agency senior staff component and/or command level element that provides staff supervision and oversight of COMSEC operations, policy establishment, procedures, accounting, resource management, material acquisition, and training throughout the department or agency. The multitude of responsibilities inherent to the COMSEC service authority functions may be allocated to one or more senior staff elements of the department or agency, while specific oversight and execution of selected functional responsibilities may be delegated to subordinate field agencies or activities within that department or agency. See also CCI central authority and service authority.

Communications security software
Includes all types of COMSEC material except key in electronic or hard copy form. This includes all classifications of unencrypted software and all associated data used to design, create, program, or run that software. It also includes all types of source, executable, object code, and associated files that implement, execute, embody, contain, or describe cryptographic mechanisms, functions, capabilities, or requirements. COMSEC software also includes transmission security software and may include any software used for purposes of providing confidentiality, integrity, authentication, authorization, or reliability service to information in electronic form.

Controlled cryptographic item
Secure telecommunications, information handling equipment, or associated cryptographic component that is unclassified but governed by a special set of control requirements. Such items are marked "controlled crytographic item" or, where space is limited "CCI".

Controlled inventory item
Items with characteristics requiring special identification, accounting, security, or handling to ensure their safeguard.

These items in order of degree to which controls may be exercised are: (1) classified items; (2) sensitive items assigned CIICs on the AMDF (CCI is assigned CIIC–9); and (3) pilferable items also assigned a CIIC on the AMDF.

Courier
Used (as a verb) interchangeably with "carry" to denote a method of conveyance that allows personal custody or control of the material while in transit. The term does not include users who must carry material from point A to point B for their own operational use.

Note. For purposes of this instruction, "courier", as a noun, refers to a person who receives material at point A and delivers it to point B.

Crypto
The marking or designator identifying unencrypted COMSEC keying material used to secure or authenticate telecommunications carrying classified or sensitive U.S. Government or U.S. Government-derived information. This includes nonsplit keying material used to encrypt and decrypt COMSEC critical software and software-based algorithms.

Crypto algorithm
Well defined procedure or sequence of rules or steps or a series of mathematical equations used to describe cryptographic processes such as encryption and/or decryption, key generation, authentication, and signatures.

Cryptonet
Stations holding a common key.

Crypto ignition key
Device or electronic key used to unlock the secure mode of crypt equipment.

Cryptosecurity
Component of COMSEC resulting from the provision of technically sound cryptosystems and their proper use.

Cryptosystem
Associated INFOSEC items interacting to provide a single means of encryption or decryption.

Declassify
An administrative action after equipment has been sanitized. Sanitization may occur when all key is zeroized and red volatile memory containing key and classified software is actively cleared. Such a process is complete when all classified or sensitive information is expunged, erased, overwritten, deleted, or otherwise changed so that it is no longer intelligible and its release would not damage national security. Alternatively, an equipment may be administratively declassified if it is determined that the remaining (possibly classified) information within the equipment will be automatically sanitized by existing antitamper mechanisms.

Destruction
An act or omission that renders property completely useless to the point of complete loss of identity and beyond the prospect of future restoration. Within the Army the only authorized destruction facility for CCI is located at TYAD.

Direct responsibility
The obligation of a person to ensure that all Government property, for which he or she has receipted for, is properly used and cared for and that proper custody and safekeeping are provided. Direct responsibility results from assignment as an accountable officer, receipt of formal written delegation, or acceptance of the property on hand receipt.

Electronically generated key
Key produced only in nonphysical form.

Note. Electronically generated key stored magnetically (for example, on a floppy disc) is not considered hard copy key.

Embedded controlled cryptographic item
A cryptographic component that is designed and engineered to be incorporated into an otherwise unclassified communication or information processing equipment or system to form a 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 integrated CCI component cannot perform any function by itself; it obtains its power from the host equipment. An embedded CCI component may take a variety of forms, such as a module, 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.

Embedded cryptography
Cryptography that is engineered into an equipment or system; the basic function of which is not cryptographic.

Emission security
Protection resulting from measures taken to deny unauthorized individuals information derived from intercept and analysis of compromising emanations from crypto equipment and IS.

Encrypted key
Key which has been encrypted in a system approved by NSA for key encryption. This assumes the key's unencrypted associated data (for example, header or tagging information) is not sensitive. The associated data also may or may not be encrypted. If the associated data is not encrypted, the entire data package may be sensitive or even classified. The CONAUTH must make the final decision as to the sensitivity of the associated data. The term "encrypted key" used in this document to refer to a key that has been encrypted and the key's associated data (for example, header information) is not sensitive. Key encryption must employ a NSA-approved process.

Note. Encrypted data is not considered crypto.

Encryption
Whenever used in this document, the words "encrypt" or "encryption" refer to a NSA process approved for protection of the given keying material.

End item
A final combination of end products, piece parts, components, and assemblies produced and ready for its intended purpose. End items in common use include the following:

a. Class II - End items which are not considered to be principal (major) items. This includes clothing, individual equipment, tentage, tools, tool sets, administrative supplies, office furnishings, and housekeeping supplies and equipment. Such items are usually prescribed in authorization documents or common table of allowances.

b. Class VII - This class identifies major (principal) end items of equipment. Major end items include weapons, vehicles, aircraft, communications systems, automation equipment, power generation equipment, which require table of organization and equipment, TDA, or common table of allowances authorization.

Fair, wear, and tear
The loss, consumption, or impairment of appearance, effectiveness, worth, or utility of an item, rendering it unserviceable or uneconomically repairable salvage that has occurred solely because of normal and customary use of the item for its intended purpose by authorized persons.

Foreign national
A person who is not a natural born or naturalized citizen of the United States and who is not categorized as a resident alien.

Future editions
Key which has been identified for operational use in a prescribed sequence but which is held by a depot or COMSEC account and has not yet been issued to the end user. NSTISSI No. 4010 addresses issuance of several types of keying material.

Government telecommunications
Telecommunications of an employee, officer, contractor, or other entity of the U.S. Government which concern an official purpose of Government and which are transmitted over a telecommunications system owned or leased by the Government or a Government contractor.

Host equipment
Any unclassified telecommunications or information processing equipment that serves as a host for an integrated (embedded) CCI component. The host equipment may process voice, data, or record communications. Normally the CCI component is installed within the host equipment and is not readily identifiable to the user. For this reason, the serial number of the host equipment must be used for accounting and tracking purposes. The host equipment is thus designated as a CCI end item.

Information assurance
Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information security
A term developed by NSA to define all measures taken to protect classified and unclassified sensitive information within telecommunications and automation systems. INFOSEC combines COMSEC and computer security measures in this new era of automated data, information, and communications systems.

Integrated controlled cryptographic item component
A CCI component that is designed to be incorporated with an otherwise unclassified communications or information processing equipment or system for a CCI equipment of CCI system.

Inventory
Within the context of this publication, an inventory is an itemized physical count and sight verification of materiel and property on hand to verify quantity, condition, and (when required) serial numbers. When directed, inventories may include a physical count of components comprising sets, kits, outfits, systems, and other end items.

JOSEKI
JOSEKI is the name of an unclassified cryptographic algorithm, which is only used to encrypt and decrypt software algorithm implementations. JOSEKI is currently the only such algorithm in use, but other algorithms may be used for this same purpose in the future.

Key
Information (usually a sequence of random or pseudo random binary digits) used initially to set up and periodically change the operations performed in a crypto equipment for the purpose of encrypting or decrypting electronic signals, for determining electronic counter-countermeasures patterns (for example, frequency hopping or spread spectrum), or for producing other key.

Keyed condition
Refers to equipment that is fully enabled to perform its mission. When only a partial key set is loaded (for example, when the CIK containing a key split is removed or when key splits are loaded but the traffic encryption key is not loaded) the equipment is in an "unkeyed" state.

Keying material
Key, code, or authentication information in physical or magnetic form.

KSV–21 card
A high-grade CIK with built-in U.S. Government-owned encryption algorithms and public key exchange protocols designed for use with the new generation STE. Initially the card is programmed with a complete CIK and is referred to as a fill card. When associated with the STE, the CIK is split and a component of the CIK is transferred to the STE for storage. Once associated with the STE, the card is referred to as a user card.

Local purchase
The authorized acquisition through procurement of supplies and services on behalf of users by supply support activity accountable officers through designated Government contracting agencies and from commercial vendors, distributors, and manufacturers. Such purchases include acquisition of items cataloged as decentralized items of supply, in lieu of requisitioning from the wholesale distribution system. Local purchase is the direct opposite of major acquisition and National buying programs administered by DOD wholesale commodity managers and the GSA under Congressionally approved budget authorizations. Local purchase also includes the direct purchase of supplies or services by activities using the U.S. Government-wide credit card system known as the Government Purchase Card Program.

Memory clear
Term used in certain equipment when RED volatile memory is actively cleared and all or most keys are zeroized.

Mission essential and vulnerable areas
Facilities, structures, or activities within an installation or geographical area that, by virtue of their functions, are evaluated and designated by the responsible commander (or a civilian equivalent) as vital to the successful accomplishment of the activity, unit, organizational, or installation mission. This includes areas not directly essential to the operational mission, but which by nature of the function, activity, or materiel therein, are considered vulnerable to

theft, trespass, damage, or other criminal act. For purposes of this regulation, all garrison (nontactical) CCI operational and storage areas are designated MEVA. MEVA exception: Administrative offices that are not in classified or restricted areas where the only CCI in use or storage in common administrative offices are STE. Such administrative areas may be waived from designation as MEVA at the discretion of the responsible commander or civilian equivalent provided the associated CIKs or KSV–21 cards containing key are removed from the instruments and properly secured when the facility is unoccupied.

Modification of controlled cryptographic item
Any change to the electrical, mechanical, physical, hardware, or software characteristics of a COMSEC end item, component, assembly, circuit, or device is considered a modification. Modifications to COMSEC materiel are specifically prohibited except when directed by an NSA-approved modification work order and performed by trained and certified COMSEC technicians.

National information assurance partnership
Joint initiative between NSA and the National Institute of Standards and Technology responsible for security testing needs of both IT consumers and producers and promoting the development of technically sound security requirements for IT products and systems and appropriate measures for evaluating those products and systems.

National office of record
The body within the National Security Agency that provides CORs with National level guidance, assistance, and oversight and ensures that CORs adhere to published standards, methods, and procedures for protecting cryptographic material.

National Security Agency and/or Central Security Service approved
NSA and/or CSS approval may consist of 1) product certification wherein NSA and/or CSS or its designee evaluates a product and certifies that it meets defined criteria, allowing certain defined usage; or 2) product or system approval wherein NSA and/or CSS approves a set of generic solutions. In the latter case, the approved solution may consist of a combination of components. The use of this combination of components allows a user to protect information of the type specified in the NSA and/or CSS approval specification.

National security information
"Classified national security information" or "classified information" means information that has been determined pursuant to EO 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

National security system
Any information system (including any telecommunications system) used or operated by an agency or by a contractor of any agency, or other organization on behalf of an agency, the function, operation, or use of which: involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapon system; or is critical to the direct fulfillment of military or intelligence missions; or is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. Does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications) (see 44 USC 3542).

Need-to-know
A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

Negligence
An act, omission, or instance when an individual fails to exercise the care of a prudent person. Within the concept of responsibility for safeguarding Army property, there are 2 legally defined categories of negligence used in making determinations of pecuniary liability. The categories are as follows:

a. Simple negligence. The failure to act as a reasonably prudent person would have acted under similar circumstances

b. Gross negligence. An extreme departure from the course of action to be expected of a reasonably prudent person, all facts and circumstances being considered, and accompanied by a reckless, deliberate, or wanton disregard for the foreseeable consequences of the act.

Open storage
Storage of classified information within an approved COMSEC facility (for example, a secure room) but not locked in a GSA-approved security container during periods of time when the facility is unoccupied by authorized personnel.

Personal identification numbers
A series of letters, special characters, and numbers known only to authorized persons used to enable access to the secure functionality of COMSEC products and/or equipment.

Personal property
Federal Government property of any kind, except for real property (land, roads, grounds, and structures) or records.

Personal responsibility
The obligation of a person to exercise reasonable and prudent actions to properly use, care for, and safeguard all Government property in his or her possession. This applies to all Government property issued to, acquired for, or converted to a person's exclusive and personal use.

Physical key
Also known as hard-copy key. Keying material such as printed key lists; punched or printed key tapes; or programmable, read-only memories.

Note. Electronically generated key stored magnetically (for example, on a floppy disc) is not considered physical key.

Positive control material
Generic term referring to a sealed authenticator system, permissive action link, coded switch system, positive enable system, or nuclear command and control documents, material, or devices.

Premature exposure of key
The removal of key from its protective packaging prior to the effective date of the key.

Note. Key that has been removed from its protective packaging in order to be loaded into a DTD is not considered to be prematurely exposed.

Property book officer
A person officially appointed in writing by proper authority to maintain formal accounting records of Government property below the retail support level, regardless of whether the property is in their possession for use or storage, or is in the possession of other responsible individuals to whom the property has been legitimately entrusted for use, or for care and safekeeping on memorandum hand receipt.

Protected Distribution System
Wire-line or fiber optic distribution system used to transmit unencrypted classified National Security Information through an area of lesser classification or control.

Qualified technician
An individual who satisfies the training requirement of NSTISSI No. 4000 and is authorized to perform a specified level of maintenance on CCIs.

Real property
Lands, buildings, structures, utilities systems, improvements, and appurtenances (property right-of-ways) thereto. Real property includes equipment permanently attached to and made part of buildings and structures, such as heating and/or air conditioning systems, but does not include movable plant equipment.

Responsibility
The obligation of an individual to ensure that Government property and funds entrusted to their possession, command, or supervision are properly used and cared for and that proper custody and safekeeping are provided. There are 4 types of responsibility as defined in this glossary:

a. Command responsibility.
b. Direct responsibility.
c. Supervisory responsibility.
d. Personal responsibility.

Risk analysis and/or assessment
Risk is defined as the chance or likelihood that an undesirable event will occur resulting in personal injury or casualties, unauthorized access or possession of classified and sensitive materiel, or the loss, damage, or destruction of

personal or real property. Within the Army, risk analysis is defined as the assessment of risk factors, threat levels, and risk values, using a standard method of examination. This assessment will be used by commanders and cognizant security authorities to decide upon the appropriate level of security measures warranted for the protection of personnel and materiel resources.

Security awareness training
A mandatory program of instruction required of all trained maintenance personnel assigned or performing any level of maintenance on any item of COMSEC equipment, systems employing COMSEC or cryptographic functions (CCI), or any equipment containing cryptographic components. COMSEC security awareness training must be provided to all such technicians, regardless of military occupational specialty and presented at a level commensurate with the maintenance technician's involvement with the equipment or system. Satisfactory completion of the training will be recorded on DD Form 2625. Required topics in the program of instruction are listed in NSTISSI No. 4000.

Sensitive item
Materiel requiring a high degree of protection and safeguards to prevent unauthorized acquisition, access, theft, or diversion and use. This includes classified items, arms, ammunition, explosives, drugs, precious metals, and CCI. Sensitive items are assigned CIICs on the AMDF (see controlled inventory item).

Service authority
DOD component-level organization that performs COMSEC activity functions in support of the central office of record. Service authority activities include oversight of COMSEC operations, policy, procedures, and training. Service authority roles may include cryptographic hardware management and distribution control; approving account establishments; approving authority for certifications approval authorities; implementing CMCS and KMI policies and procedures; direct operational support; final adjudication authority for determining when reported COMSEC incidents result in COMSEC insecurities; and ensuring Service compliance with COMSEC access program requirements (see COMSEC service authority).

Superseded key
A key that has been replaced with a different edition or segment. The scheduled supersession of key is based on its cryptoperiod. The unscheduled supersession of key is directed by the CONAUTH. So-called "used" key (for example, key tape segments that have been loaded into a DTD) is not superseded simply because it has been loaded into an electronic fill device. It remains current operational or in some cases, future key until it reaches the end of its cryptoperiod.

Supervisory responsibility
Obligation of a supervisor to ensure that all Government property issued to, or used by, his or her subordinates is properly used and cared for, and that proper custody and safekeeping of the property are provided. It is inherent in all supervisory positions and is not contingent upon signed receipts or responsibility statements. It arises because of assignment to a specific position and includes the following:

a. Providing proper guidance and direction.
b. Enforcing all security, safety, and accounting requirements.
c. Maintaining a supervisory climate that will facilitate and ensure the proper care and use of Government property.

Supply support activity
A formally established MTOE or MTOE retail support activity assigned a supply mission in support of user customer supply accounts and maintenance repair or overhaul missions. Supply support activities are established at direct support, general support, and installation levels. They maintain stockage inventories of support items consistent with commander-approved authorized stockage lists based on customer demands, mission essentiality, and other authorized or approved stockage criteria, depending on criticality of assigned missions, as directed by higher authority.

The Army Authorization Document System
An automated system that supports the development and documentation of organizational structures and the requirements for an authorization of personnel and equipments needed to accomplish assigned mission of Army units and activities. It is the basis for approval and publication of Army table of organization and equipment, MTOE, TDA, and common table of allowance authorization documents.

Tier 0
Composite of NSA's Fort Meade and Finksburg key facilities providing centralized key management services for all forms of key.

Tier 1
The layer of the EKMS which serves as the intermediate key generation and distribution center, central office of record, privilege manager, and registration authority for EKMS Tier 2 accounts.

Tier 2
The layer of the EKMS comprised of the COMSEC accounts managing key and other COMSEC material.

Tier 3
The lowest tier or layer of the EKMS architecture which includes the DTD SKL and all other means used to transfer key to cryptographic equipment.

Transmission security
Component of COMSEC resulting from the application of measures designed to protect transmissions from interception and exploitation by means other than crypto analysis.

Transportation officer
The officer responsible to the installation commander for shipment of property. This individual initiates and processes bills of lading, transportation control movement documents, and other manifests to affect the movement of Government equipment, supplies, and property.

Two-person control
Continuous surveillance and control of positive control material at all times by a minimum of 2 authorized individuals, each capable of detecting incorrect and unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements.

Two-person integrity
System of storage and handling designed to prohibit individual access to certain COMSEC keying material by requiring the presence of at least 2 authorized individuals, each capable of detecting incorrect or unauthorized security procedures with respect to the tasks being performed.

Used physical key
Key tape segments that have been removed from their canisters and used to load an electronic fill device are referred to as “used” key. This does not mean that the key is superseded. It remains operational or in some cases future key until it reaches the end of its cryptoperiod. Unless the system security doctrine for the key states otherwise, these segments should be destroyed immediately after a successful load has been attained. The duplicate segments may be maintained (for example, for use in “cold start” situations), at the discretion of the user or the CONAUTH until scheduled supersession of the key occurs.

U.S. Government contractor
An individual, corporation, partnership, association, or other entity performing work under a U.S. Government contract either as a prime contractor or as a subcontractor.

User representative
Person authorized by an organization to order COMSEC keying material and to interface with the keying system to provide information to key users, ensuring that the correct type of key is ordered.

Wholesale level
The level of logistics support providing supply, maintenance, transportation, and acquisition (procurement) services to DOD military departments and agencies. They include, national inventory control points, national maintenance points, depots, terminals, ports, arsenals, central wholesale data banks, plants, factories, and Government contractor facilities associated with commodity command activities; and other specifically designated special Army activities above the retail level retained under direct control of HQDA or designated ACOM, ASCC, or DRU. Wholesale functions are most commonly performed in the U.S. and its territories and possessions. However, during mobilization and major contingency operations, wholesale operations such as terminals, ports, and depot activities may be established in an overseas theater of operations to support forward deployed field armies. A wholesale support system procures supplies and services for the Army from commercial sources or from Government plants. Wholesale supply support is normally accomplished by distributing supplies to retail level support activities for stockage and issue to users. However, during contingencies and major distribution programs for new weapons systems, total package fielding, and other distribution actions may be made directly from wholesale sources to operational combat and combat support commands.

Zeroize
To remove or eliminate the key from a crypto equipment or fill device.

Section III
Special Abbreviations and Terms

IAT
Information Assurance Technical

MEVA
mission essential and vulnerable areas

NSI
National Security Information

NSTISSP
National Security Telecommunications and Information Systems Security Policy

PIN 004087–000