ATP 6-02.75

TECHNIQUES FOR COMMUNICATIONS SECURITY

MAY 2020

This publication supersedes ATP 6-02.75, dated 17 August 2015.

Headquarters, Department of the Army

This publication is available at the Army Publishing Directorate site (https://armypubs.army.mil/) and the Central Army Registry site (https://atiam.train.army.mil/catalog/dashboard).

*ATP 6-02.75

Army Techniques Publication
No. 6-02.75

Headquarters
Department of the Army
Washington, DC, 18 May 2020

Techniques for Communications Security

Contents

*This publication supersedes ATP 6-02.75, dated 17 August 2015.

Figures

Tables

Preface

ATP 6-02.75 expands on the discussion of communications security in FM 6-02. This publication establishes non-prescriptive ways or methods for performing communications security planning, employment, handling, and use. This publication also provides an overview of the key management infrastructure used to generate, distribute, and account for communications security materials.

The primary audience for ATP 6-02.75 is commanders, staffs, supervisors, and users of communications security devices and material. Communications security account managers and other personnel involved in planning, management, and communications security accounting adhere to the policies and procedures in AR 380-40 and TB 380-41. Readers should be familiar with ADP 1, ADP 3-0, FM 3-0, and FM 6-02 to correctly apply this doctrine.

Commanders, staffs, and subordinates ensure that their decisions and actions comply with applicable United States, international, and, in some cases, host-nation laws and regulations. Commanders at all levels will ensure their Soldiers operate in accordance with the law of armed conflict and applicable rules of engagement. (See FM 6-27.)

ATP 6-02.75 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. For definitions shown in the text, the term appears in italics, and the number of the proponent publication follows the definition. This publication is not the proponent for any Army terms.

ATP 6-02.75 applies to the Active Army, Army National Guard/Army National Guard of the United States, United States Army Reserve unless otherwise stated.

The proponent of this publication is the United States Army Cyber Center of Excellence. The preparing agency is the Doctrine Division, United States Army Cyber Center of Excellence. Send comments and recommendations on DA Form 2028 (*Recommended Changes to Publications and Blank Forms*) to Commander, United States Army Cyber Center of Excellence and Fort Gordon, ATTN: ATZH-OP (ATP 6-02.75), 506 Chamberlain Avenue, Fort Gordon, GA 30905-5735; by e-mail to usarmy.gordon.cyber-coe.mbx.gord-fg-doctrine@mail.mil.

This page intentionally left blank.

Introduction

"A strong case can be made that, seen broadly, a major purpose of COMSEC—perhaps its overriding purpose—is to help achieve surprise by denying adversaries and enemies foreknowledge of our capabilities and intentions."

David G. Boak

Commanders surprise enemy forces by attacking at a time or place or in a manner for which enemy forces did not prepare for or expect. Commanders achieve surprise by showing enemy forces what they expect to see while actually doing something different. Surprise delays enemy reactions, overloads and confuses enemy command and control systems, induces psychological shock, and reduces the coherence of an enemy force's defense (ADP 3-90).

Understanding the risk of surprise, enemies and adversaries will undertake intelligence activities to determine U.S. intentions. Operation plans are most vulnerable to enemy discovery through communications and information systems.

Communications security hardware and software help preserve the element of surprise in operations by protecting sensitive information from enemy and adversary intelligence efforts. Communications security devices and techniques preserve the confidentiality, integrity, and availability of U.S. communications and information systems against enemy attempts at interception, spoofing, manipulation, or jamming.

Communications security measures must balance the need to maintain security with the need to effectively access and use the network and network resources for planning and communications. Department of Defense networks use robust encryption capabilities to protect sensitive information. The effectiveness of encryption to secure information and networks depends on controlling and accounting for cryptographic keying material so it does not become compromised.

Note. Where this ATP appears to conflict with Army communications security policy and procedures contained in AR 380-40, TB 380-41, and AR 710-2, those publications take precedence. Users of this manual should immediately report all conflicts to the United States Army Cyber Center of Excellence Doctrine Branch. (See contact information in the preface on page iii of this manual.)

ATP 6-02.75 is the primary doctrine publication for users of communications security materials. This publication consists of six chapters—

Chapter 1 introduces communications security and discusses roles and responsibilities for the Army communications security program, commander and staff responsibilities, the communications security material control system, communications security authorities, and responsibilities for civilian and military account managers.

Chapter 2 addresses cryptographic net planning and establishment, signal operating instructions, and loadset management. This chapter then discusses the Department of the Army cryptographic access program, and the importance of software upgrades and periodic tamper checks of end cryptographic units.

Chapter 3 provides an overview of key management and the key management infrastructure. It discusses various key management nodes, transfer key encryption key management, and key management levels.

Chapter 4 discusses distribution planning, over-the-air distribution, encrypted key distribution, and the Defense Courier Division. This chapter further discusses communications security considerations for joint and multinational operations and deployment COMSEC support

Chapter 5 addresses communications security material accounting, including certificate management, hand receipts, compromise recovery, incident evaluation and types, maintenance, and two-person integrity for top secret communications security materials.

Chapter 6 provides an overview of controlled cryptographic items and discusses requirements for accountability, transfer, storage, and release to foreign nationals. This chapter further discusses protective technologies, transfer of controlled cryptographic items between Services or agencies, and maintenance of controlled cryptographic items.

Chapter 1
Communications Security Overview

This chapter introduces communications security and discusses roles and responsibilities for the Army communications security program, commander and staff responsibilities, the communications security material control system, communications security authorities, and responsibilities for civilian and military account managers.

INTRODUCTION TO COMMUNICATIONS SECURITY

1-1. Maintaining secure communications is vital to command and control in military operations. Information transmitted by communications and automated information systems is vulnerable to interception and technical exploitation by enemies or adversaries. Countering interception and exploitation of communications and information systems requires that users protect sensitive classified and unclassified information during transmission.

1-2. Army networks and information systems are under relentless attack as adversaries attempt to disrupt or compromise U.S. networks and information systems. As sophisticated exploitation technology becomes more readily available, less expensive, and more mobile, adversaries expand their ability to exploit network vulnerabilities via cyber warfare.

1-3. Communications security (COMSEC) hardware and software help protect sensitive U.S. communications and data against adversary attack or exploitation. *Communications security* is actions designed to deny unauthorized persons information of value by safeguarding access to, or observation of, equipment, material, and documents with regard to the possession and study of telecommunications or to purposely mislead unauthorized persons in their interpretation of the results of such possession and study (JP 6-0). COMSEC is a cybersecurity capability, as identified in AR 25-2. COMSEC helps ensure the confidentiality, integrity, availability, and non-repudiation of Army information. The components of COMSEC are—

- ***Cryptographic security*** is the component of communications security that results from the provision of technically sound cryptographic systems and their proper use (CNSSI 4009).
- ***Transmission security*** is actions designed to protect transmissions from interception and exploitation by means other than cryptanalysis (JP 6-0). Transmission security deals with the security of communications transmissions, rather than that of the information being communicated.
- ***Emission security*** is actions designed to deny unauthorized persons information of value as a result of intercept and analysis of compromising emanations from cryptographic equipment and telecommunications systems (JP 6-0).
- ***Physical security*** is that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft (JP 3-0). The physical security component of COMSEC safeguards classified equipment, material, and documents from access or observation by unauthorized persons.

1-4. COMSEC devices and services enable secure communications in joint networked environments. Table 1-1, page 1-2 lists the rules for applying COMSEC protection to secure sensitive classified and unclassified information.

Table 1-1. Applying communications security devices to protect information

When transmitting information that is	*Secure or protect information using a*
Classified	NSA-approved solution.
A combination of classified and sensitive information.	NSA-approved solution.
Sensitive information that involves— • Intelligence activities. • Cryptologic activities related to national security. • Command and control of military forces. • Equipment that is an integral part of a weapon or weapon system. • Equipment that is critical to the direct fulfillment of military or intelligence missions.	NSA-approved solution.
Any other type of business or administrative sensitive information (such as PII, FOUO, CUI, financial, logistics, protected health information, personal or payroll information, proprietary, source selection, and personnel management) that is not considered publicly releasable.	Cryptographic module validated under the NIST cryptographic module validation program as meeting at least level 2 security requirements of FIPS PUB 140-3.

Legend:

CUI	controlled unclassified information	NSA	National Security Agency
FIPS	federal information processing standards	PII	personally identifiable information
FOUO	for official use only		
NIST	National Institute of Standards and Technology		

ROLES AND RESPONSIBILITIES

1-5. 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 (AR 380-40). The following paragraphs explain the distributed roles and responsibilities for COMSEC distribution, accountability, and maintenance.

DIRECTOR, NATIONAL SECURITY AGENCY

1-6. The Director, National Security Agency (NSA) is the national manager for national security telecommunications and information systems security. The Director, NSA is subordinate to the Secretary of Defense, who is the executive agent for the Committee on National Security Systems (CNSS). The Director, NSA establishes national level COMSEC policies. The NSA is the approval authority for COMSEC standards, techniques, equipment, and protected services for national security systems. The NSA also certifies or approves cryptographic systems and techniques used by or on behalf of DOD activities to protect national security systems and national security information.

DEPUTY CHIEF OF STAFF, INTELLIGENCE

1-7. The Department of the Army Office of the Deputy Chief of Staff, Assistant Chief of Staff, Intelligence (G-2) prescribes policies and approves procedures for safeguarding and controlling COMSEC material. The Deputy Chief of Staff, G-2 manages the Department of the Army Cryptographic Access Program, and accepts cryptographic access granted by other DOD components. Refer to AR 380-40 for a comprehensive list of COMSEC roles and responsibilities of the Deputy Chief of Staff, G-2.

CHIEF INFORMATION OFFICER/ASSISTANT CHIEF OF STAFF, SIGNAL

1-8. The Department of the Army Chief Information Officer (CIO)/Assistant Chief of Staff, Signal (G-6) establishes policy, resourcing, and oversight of the Army cybersecurity program and issues policies and guidance for Army cybersecurity activities. The CIO/G-6 sets the strategic direction and policy for Army-wide activities to ensure confidentiality, integrity, and availability of the network.

1-9. The CIO/G-6 oversees operational implementation of the Army COMSEC program, including enforcement of COMSEC policies, directives, criteria, standards, and doctrine. The CIO/G-6 Cybersecurity Directorate determines which COMSEC material, controlled cryptographic items, and cryptographic high-value property are approved for use on Army networks.

Note. Army cybersecurity program resources are located on the Army Cybersecurity One Stop Shop portal.

COMMUNICATIONS SECURITY LOGISTICS ACTIVITY

1-10. The Communications Security Logistics Activity (CSLA) manages systems and programs for cryptographic key management and distribution. The CSLA support team assists with technical and logistics inquiries that a key management infrastructure operating account manager (KOAM) may have concerning COMSEC policy and related issues. The CSLA operates a 24-hour emergency operations center.

1-11. The CSLA conducts audits and inspections to certify and validate accountability, safeguarding, and control of COMSEC material. The CSLA audits and inspects Army COMSEC accounts every 24 months. CSLA auditors announce audits and inspections approximately 45 days in advance, and obtain approval from the controlling authority (CONAUTH) and the commander before inspecting an account. The CSLA may conduct unannounced audits and inspections, based on security and accountability issues. Audits and inspections include inventorying all accountable COMSEC material and an examining—

- Physical security measures in effect.
- COMSEC material management.
- The record of the last command COMSEC inspection and CSLA audit and inspection.
- Accounting records.

1-12. The CSLA's quarterly COMSEC Logistics and Technical Newsletter provides an informal source of information regarding COMSEC equipment, policy, training, events, and program updates. The primary target audience of the newsletter are account managers, property book officers, maintenance personnel, and controlled cryptographic item serialization managers. Other worldwide customers, including those from other Services, also use this newsletter. The newsletter is available on the CSLA Website.

1-13. The CSLA has information security representatives located worldwide to assist account managers. Information security representatives provide clarification on training, policy, doctrine, maintenance standards, and accounting requirements. The CSLA provides logistics assistance to customers that manage COMSEC equipment and material. The CSLA help desk provides technical support to account managers. The CSLA Website shows a map with the geographic alignment and current contact information for CSLA information security representatives.

COMMANDERS AND STAFFS

1-14. Commanders carry the responsibility of safeguarding and controlling COMSEC material in their units to ensure its continuous integrity and prevent access by unauthorized persons. Safeguarding and controlling COMSEC material is also the responsibility of individuals in possession of the material.

1-15. For each COMSEC account under their authority, the commander appoints a primary and one or more alternate account managers who meet the training and security clearance requirements. Commanders may delegate signature authority to subordinates, but not overall responsibility or decision authority. Once the commander identifies personnel to manage the COMSEC account, the unit training manager schedules

training for KOAM certification. Certification as a KOAM requires completion of the COMSEC account manager course and the management client course.

1-16. In accounts that maintain top secret COMSEC material, commanders appoint a primary KOAM and three alternates to maintain the account, make decisions, enforce regulatory compliance, and maintain two-person integrity. Commanders may appoint more than the minimum number of alternates to ensure account stability in case of an unexpected absence of account managers.

1-17. Commanders establish a unit COMSEC standard operating procedure (SOP). The SOP includes risk assessments to establish and document security measures for all COMSEC material and controlled cryptographic items The risk management framework allows commanders to monitor security controls and determine the security impact of changes to Army networks and the information environment. The unit COMSEC SOP should include—

- Unit-specific instructions.
- Routine destruction instructions.
- Controlled cryptographic item management instructions.
- Deployment instructions.
- Emergency plan instructions.
- Continuity of operations plan.
- Information technology contingency plan.

Note. Refer to DODI 8510.01 for more information about applying the risk management framework to COMSEC materials.

Corps and Division

1-18. The corps and division G-6s are responsible for COMSEC account management and logistical readiness oversight at their respective echelons. When a corps or division headquarters serves as a joint task force headquarters, the G-6 oversees joint COMSEC activities.

1-19. The corps and division KOAMs are members of the network operations and security center staff. Corps and division KOAMs order, receive, account for, and distribute COMSEC material, including storing encrypted keys, generating keys, performing electronic key distribution.

Brigade

1-20. Brigade KOAMs perform the same duties as their corps and division counterparts. The battalion or brigade signal staff officer (S-6) provides oversight and coordination of COMSEC operations, including storage, management, distribution, inspection, and compliance. Additional S-6 COMSEC responsibilities include—

- Advising the commander on COMSEC activities.
- Planning and coordinating distribution and use of COMSEC materials.
- Collaborating with higher headquarters G-6 or the communications system directorate of a joint staff on COMSEC activities.
- Overseeing brigade COMSEC accounts and other COMSEC-related matters.

COMMUNICATIONS SECURITY MATERIAL CONTROL SYSTEM

1-21. The *communications security material control system* (CMCS) is the logistics and accounting system through which communications security material marked CRYPTO is distributed, controlled, and safeguarded. Included are the communications security central offices of record, cryptologistic depots, and communications security accounts. Communications security material other than key may be handled through the communications security material control system. Electronic Key Management System and key management infrastructure are examples of tools used by the communications security material control system to accomplish its functions (CNSSI 4005). The CMCS consists of—

- COMSEC accounts.
- COMSEC central office of record.
- Depots.
- Policies, procedures, and accounting systems to account for and protect the security of COMSEC material.

1-22. Army customers submit validated COMSEC requirements to the CSLA through property book channels. Customers can request unclassified and classified COMSEC equipment authorized by their unit's modified table of organization and equipment or table of distribution and allowances through the CSLA Website. Upon approval of the request, the CSLA releases the equipment through the CMCS or logistics channels. The CMCS accounts for keying material, classified COMSEC equipment, and COMSEC publications assigned an accounting legend code (ALC) by the NSA.

1-23. An *accounting legend code* is a numeric code used to indicate the minimum accounting controls required for items of accountable communications security material within the communications security material control system (CNSSI 4009), The account manager inventories ALC 1, 2, and 6 COMSEC materials every six months and reconciles the inventory with the central office of record. The account manager inventories ALC 4 and 7 COMSEC materials annually and during a change of KOAM. Table 1-2 outlines reporting requirements for the different ALCs. Refer to AR 380-40 for more details on CMCS.

Table 1-2. Accounting legend codes and reporting requirements

Accounting legend code	*Reporting requirements*
ALC 1	Accountable to the COR by serial number.
ALC 2	Accountable to the COR by quantity.
ALC 4	Not accountable to the COR but the KOAM accounts for this material locally until final disposition.
ALC 6	Electronic keys generated by account workstation. Although a capability exists at the KOA, Army units will not generate ALC 6 keying material.
ALC 7	Electronic keys generated by account workstation and locally accountable until final disposition.
Legend: ALC accounting legend code COR central office of record KOA key management infrastructure operating account KOAM key management infrastructure operating account manager	

***Note*.** Account managers report ALC 1, 2, and 6 materials to the central office of record and ALC 4 and 7 materials locally.

AUTHORITIES

1-24. COMSEC authorities vary according to responsibilities and assignments. Commanders appoint personnel with specific authorities to make decisions and enforce compliance with COMSEC policies and procedures within their command.

SERVICE AUTHORITY

1-25. The service authority is the senior staff component or command-level element in each military Service that provides staff supervision and oversight of COMSEC operations, policies, procedures, accounting,

resource management, materiel acquisition, and training throughout the department or agency. Commanders assign one or more senior staff elements of their Department or agency to fulfill service authority responsibilities. Commanders may delegate oversight and execution of selected functional responsibilities to subordinate field agencies and activities.

COMMAND AUTHORITY

1-26. The *command authority* (CMDAUTH) is responsible for the appointment of user representatives for a department, agency, or organization and their key and granting of modern (electronic) key ordering privileges for those user representatives (CNSSI 4005). In an Army unit, the CMDAUTH should be organizationally senior to user representatives and have the knowledge and expertise to perform essential management functions.

CONTROLLING AUTHORITY

1-27. The *controlling authority* is the official responsible for directing the operation of a cryptographic net (cryptonet) using traditional key and for managing the operational use and control of keying material assigned to the cryptonet (CNSSI 4009). A cryptonet consists of stations holding a common key. A single cryptonet may include multiple communications networks.

1-28. The commander may delegate CONAUTH responsibilities in writing to a trusted subordinate technically qualified to perform these duties. However, responsibility for fulfillment of CONAUTH responsibilities rests with the commander. CONAUTH responsibilities include—

- Initiating recovery and reconstitution actions.
- Authorizing key replacement and resupply.
- Directing classification changes for a key.
- Establishing a cryptographic period and approving extensions (refer to DA PAM 25-2-16).
- Specifying implementation and supersession dates for a key.

COMMUNICATIONS SECURITY ROLES

1-29. Managers at all levels enforce security measures to ensure the protection of DOD property, national security information, and personnel. The commander may assign personnel several key management infrastructure (KMI) roles in order to perform all COMSEC functions. While COMSEC accounting is centralized, individual users hold keying material and devices at the lowest echelon that can maintain adequate physical security. This allows managers and operators to react to contingencies such as emergency key supersession, equipment failure, or operator error, with minimal downtime.

KEY MANAGEMENT INFRASTRUCTURE OPERATING ACCOUNT MANAGER

1-30. A *key management infrastructure operating account manager* is an external operational management role that is responsible for the operation of a key management infrastructure operating account that includes all distribution of key management infrastructure key and products from the management client to the end cryptographic units and fill devices, and management and accountability of all electronic and physical key, and physical communications materials from receipt and/or production to destruction or transfer to another key management infrastructure operating account. (Similar to an electronic key management system manager or communications security account manager.) (CNSSI 4005).

1-31. The KOAM is responsible for the receipt, custody, security, accountability, safeguarding, inventory, transfer, and destruction of COMSEC material. The KOAM oversees local elements to ensure compliance with policies and procedures for security, accounting, acquisition, control, and distribution of COMSEC material. Refer to TB 380-41 for detailed responsibilities of the KOAM.

ALTERNATE KEY MANAGEMENT INFRASTRUCTURE OPERATING ACCOUNT MANAGER

1-32. An alternate KOAM performs the same duties as the primary. The primary account manager or commander assigns these duties to the alternate account managers. The alternate KOAM must be aware of the

day-to-day operations of the account and be able to perform required duties when the primary is not available. Commanders should appoint multiple alternates to maintain account coverage during continuous operations. The alternate KOAM helps maintain continuity of the account in case of emergencies or unexpected events.

1-33. The primary and alternate account managers must complete the COMSEC account manager course and the management client course before their appointment. Commanders appoint primary and alternate account managers according to the grade requirements in table 1-3.

Table 1-3. Grade requirements for primary and alternate key management infrastructure operating account managers

Individuals appointed as a(n)	*Grade requirement*
Key management infrastructure operating account manager	Commissioned officer, warrant officer, enlisted E-6 or above, or a civilian GS-7 or above.
Alternate key management infrastructure operating account manager	Military E-5 or above or a civilian GS-5 or above. A contractor.
Legend: GS general schedule	

Note. Government contractors may appoint personnel to serve as primary and alternate KOAMs when authorized to establish and operate Army COMSEC accounts under the terms of U.S. Government contracts. Contractors must hold comparable grades to government personnel as listed on DD Form 254 (*Department of Defense Contract Security Classification Specification*). Contractors must adhere to the guidelines in AR 380-40, TB 380-41, and DOD 5220.22M.

CLIENT PLATFORM ADMINISTRATOR

1-34. The client platform administrator performs system administration and troubleshooting of the management client (MGC). Assignment as client platform administrator requires Information Assurance Technical level-1 certification and a security clearance at the same classification level as the account or higher. Client platform administrator may be an additional assigned role of the primary or alternate KOAM or assigned to a person external to the account. Personnel assigned only client platform administrator duties have no minimum grade requirement, do not require the completion of the COMSEC account manager course, and may be contractors.

CLIENT PLATFORM SECURITY OFFICER

1-35. The client platform security officer is responsible for basic input/output system configuration for COMSEC devices, and for archiving and storing system audit data. The client platform security officer cannot hold any other KMI roles. Client platform security officer duties require minimal account interaction. There is no minimum rank requirement and no requirement for the client platform security officer to complete the COMSEC account manager course. Contractors are eligible to fill the client platform security officer position. Performance of these duties requires that the client platform security officer have—

- Information Assurance Technical level-1 certification.
- The same level security clearance as the account or higher.
- Completion of the computer-based training for their respective roles.

USER REPRESENTATIVE

1-36. A *user representative* is the key management entity authorized by an organization and registered by the Central Facility Finksburg to order asymmetric key (including secure data network system key and

message signature key) (CNSSI 4005). The user representative or product requester is the person authorized by the CMDAUTH to order COMSEC keying material. The user representative or product requester who interfaces with key managers at a central facility orders COMSEC material. The user representative informs the KOAM of keying material they have requested.

1-37. The user representative may be the KOAM, since they have access to the KMI workstations. There may be situations where the user representative is not a KOAM. Some user representatives, such as contractors, do not operate or have access to KMI workstations. These user representatives work directly with the central facility to determine their method of operation.

END USER

1-38. End users protect COMSEC material under their control and report anything that could jeopardize the COMSEC material. Users follow the KOAM's instructions for protecting and controlling COMSEC material. Users also comply with instructions provided by the property book officer for controlling and safeguarding controlled cryptographic items.

Chapter 2
Cryptographic Net Planning

This chapter addresses cryptographic net planning and establishment, signal operating instructions, and loadset management. This chapter then discusses the Department of the Army cryptographic access program, and the importance of software upgrades and periodic tamper checks of end cryptographic units.

CRYPTOGRAPHIC NET OVERVIEW

2-1. Security in networks and system devices is essential to protect the information carried by the network. Cryptographic keys enable secure encryption and decryption of the voice and data passed through transmission devices and computers. The NSA controls most encryption keys and governs local key generation, distribution, and storage.

2-2. The CONAUTH considers which type of cryptonet is most beneficial for the unit and establishes cryptonet configurations at the minimum operational size necessary for the mission. Examples of cryptonet types include point-to-point links, local area networks, wide area networks, satellite circuits, and single-channel radio networks. The CONAUTH determines how many keys to issue to users. The CONAUTH determines requirements based on the types of organizations requesting electronic key distribution support. Process security doctrine publications define the national policy on types of keys, cryptonet size, cryptographic periods, and key changeover times.

PLANNING

2-3. The corps and division G-6s work closely with the higher headquarters G-6 or joint communications staff directorate, subordinate S-6 officers, and the corps and division signal, intelligence, and sustainment companies to achieve integrated network management and network services aligned with the commander's intent. Planning a cryptonet involves identifying operational requirements in a command or unit. Corps and division G-6 network managers plan networks consisting of transmission systems, circuit switches, data switches, routers, and other devices.

2-4. Network planners develop a communications plan to support the unit's operation plan or order. The planner bases the cryptonet plan on the communications plan. Network managers consider—

- The mission objective.
- Units that will participate in the mission.
- Communications required for the mission.
- Duration of the mission.
- Other areas of mission interest.

2-5. The network planner develops a cryptonet overlay and identifies COMSEC requirements for the mission based on the operation order and communications plan. The Automated Communications Engineering Software (ACES) workstation provides the ability to tailor the software to meet a variety of planning requirements. The ACES software includes a planning module for each network category. The categories of network plans supported by ACES include—

- Warfighter Information Network-Tactical.
- Combat net radio.
- General-purpose networks.
- Adaptive networking wideband waveform.

2-6. For a cryptonet to communicate securely, all members of the net must use compatible equipment and keying material. The MGC processes cryptographic key requirements based on operator input. The KOAM provides the network planner the short title information for each key to add to the cryptonet overlay. When the plan is complete with the short titles, the KOAM returns the cryptographic plan to the network planner. The network planner finishes processing the cryptonet and provides the cryptonet plan, signal operating instructions (SOI), and loadset data to local end users. The KOAM generates and distributes the red key to end users by loading keys into the users' fill devices. Users load the end cryptographic units using a fill device.

SIGNAL OPERATING INSTRUCTIONS AND LOADSET MANAGEMENT

2-7. The corps G-6 network planner either generates and disseminates the SOI and loadset data or delegates those responsibilities to subordinate divisions. G-6 COMSEC personnel generate SOI data, COMSEC data, frequency hopping data, corps-wide hopsets, network identity, and the corps' traffic encryption key.

2-8. Division G-6 COMSEC personnel use the corps-generated data. Division G-6 COMSEC personnel generate their own frequency hopping and COMSEC data, if authorized. The division has the equipment and capability to generate and merge SOI data. The division G-6 can also generate frequency hopping data, network identity, a division TEK, and transmission security key (TSK).

2-9. Echelons brigade and below do not normally generate SOIs, TEKs, TSKs, or network identity assignments. The exceptions are when brigade and below operators are authorized to generate TEKs to meet emergency requirements. When lower echelons generate TEKs, they process them through their higher headquarters to the CONAUTH for consolidation.

2-10. The brigade receives SOI, frequency hopping, and COMSEC data from the division G-6. The brigade is primarily responsible for SOI data and preparing loadsets. The brigade tailors the SOI to its requirements, generates company-level TEKs, and develops loadsets. A loadset consists of COMSEC key tags, hopsets, lockouts and target definition, TSK, and net identifier.

2-11. Battalion and below responsibilities are limited to distributing SOI data, distributing loadsets (including Zulu time), and loading data into radios. Most echelons can distribute frequency hopping and COMSEC data through either physical or electronic means.

2-12. COMSEC personnel generate mission-specific TSKs and disseminate them through spectrum managers to the supporting forces. KOAMs coordinate key requirements and produce a COMSEC callout message to identify keys for joint, theater army, corps, or division use. As the theater army and subordinate units identify network requirements, they compile a master network list.

CRYPTOGRAPHIC ACCESS PROGRAM

2-13. All federal agencies using cryptographic devices and classified cryptographic information require a cryptographic access program. In situations where the Army provides COMSEC support to another DOD Service or agency, or to a non-DOD U.S. Government agency, the KOAM requests a statement from the supported agency verifying that they are in compliance with the cryptographic access requirements of CNSS Policy No. 3. If the KOAM cannot obtain this verification, they immediately notify the Deputy Chief of Staff, G-2, with an information copy to the CSLA and request guidance (AR 380-40). The G-2 or battalion or brigade intelligence staff officer administers the unit cryptographic access program. The program includes—

- Cryptographic access briefings.
- Coordination with the Army Intelligence Polygraph and Credibility Assessment Program Manager to ensure persons enrolled in the Department of the Army Cryptographic Access Program are subject to a random counterintelligence scope polygraph.
- Execution of cryptographic access certificates.
- Maintaining records on all individuals who have been granted cryptographic access or have had their cryptographic access withdrawn.
- Retention of cryptographic access certificates or legally enforceable facsimiles in accordance with Army records disposition schedules.

- Denying or withdrawing cryptographic access to those individuals who fail to agree to, or comply with, the criteria identified in AR 380-40, to include those enrolled in the Department of the Army Cryptographic Access Program who refuse to take a random counterintelligence scope polygraph.
- Incorporate this unit cryptographic security program into appropriate training and awareness programs.

END CRYPTOGRAPHIC UNIT INTERFACES

2-14. An end cryptographic unit is a device that encrypts and decrypts data passed over the network. The end cryptographic unit implements the electronic key at the end-user level. Interfaces include internal, MGC operator, system administrator, and external. The end cryptographic unit exchanges data with the MGC through the serial interface. These interfaces give the account manager the capability to distribute cryptographic keys to the user either in person or over a secure telephone connection.

END CRYPTOGRAPHIC UNIT SOFTWARE UPGRADE PLANNING

2-15. A software upgrade may be required for compatibility, to enhance function, or to meet mission needs. Mandatory software upgrades are normally available for download from the manufacturer's website. Maintaining current software versions ensures compatibility and continued operation. The Army Cryptographic Modernization Website maintains roadmaps of planned software upgrades and releases by equipment family and type. In joint operations where other Services may use different software versions, Army CONAUTHs determine which upgrades to implement and when in order to minimize disruptions.

2-16. The four avenues for outside assistance are—

- The Army KMI Help Desk—
  - Commercial (877) 896-8094.
  - Defense Switched Network (312) 879-9900.
- Army Key Management Website.
- Item manager.
- Vendor customer support.

UPGRADE NOTIFICATIONS

2-17. Units receive update notifications by—

- Department of the Army standard message format.
- COMSEC logistics and technical bulletin announcement.
- Program management office website announcement.

Note. Vendor software upgrades may require additional coordination through a COMSEC account after approval from the software engineering center.

This page intentionally left blank.

Chapter 3
Key Management

This chapter provides an overview of key management and the key management infrastructure. It discusses various key management nodes, transfer key encryption key management, and key management levels.

OVERVIEW

3-1. *Key management* is the activities involving the handling of cryptographic keys and other related security parameters (e.g. passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and destruction (CNSSI 4009). Key management refers to the management of cryptographic keys in a cryptographic system. Cryptographic systems provide a single means of encryption and decryption. Successful key management is critical to the security of a cryptographic system. Key management involves user training, system policies, organizational interactions, and bringing together all these elements to maintain secure communications.

3-2. A key management system generates, distributes, and manages cryptographic keys for devices and applications. This system may cover all aspects of security from secure generation of keys, secure exchange of keys, to secure key handling and storage on the client workstation. A key management system includes functions for key generation, distribution, and replacement, as well as client functionalities for injecting, storing, and managing keys on devices.

KEY MANAGEMENT INFRASTRUCTURE

3-3. *Key management infrastructure* is the framework and services that provide the generation, production, storage, protection, distribution, control, tracking, and destruction for all cryptographic keying material, symmetric keys as well as public keys and public key certificates (CNSSI 4005). KMI provides a unified, interoperable, and trusted infrastructure for establishing, using, operating, and managing cryptographic products and services in a net-centric environment. KMI provides an enterprise-wide ability to order, manage, deliver, and monitor the status of cryptographic products. KMI manages cryptographic keying material, symmetric keys, public keys, and public key certificates and supports all command elements across the army enterprise.

COMMERCIAL COMMUNICATIONS SECURITY ENDORSEMENT PROGRAM

3-4. The Commercial Communications Security Endorsement Program establishes a relationship between the NSA and industry, in which the NSA provides the COMSEC expertise. Industry provides design, development, and production capabilities to produce a cryptographic device to secure telecommunications, information handling, and computer systems. Products developed under the Commercial Communications Security Endorsement Program may include modules, printed circuit boards, microcircuits, subsystems, equipment end items, complete systems, or ancillary devices.

OBJECTIVES

3-5. KMI provides key management services and cryptographic products to users and devices to enable secure communications. The objectives for KMI are—

- Provide a secure net presence for KMI key management.
- Enable customer transition from the Electronic Key Management System.

- Provide web-based key ordering and distribution, enrollment, accounting, and compromise recovery for all key types.
- Provides over-the-network-keying for KMI-aware end cryptographic units and KMI client nodes.

ROLES

3-6. KMI manager roles provide access controls and enable managers to perform a prescribed set of activities based on manager role and system privileges. A KMI manager may have privileges in multiple roles. KMI uses a role-based operations process where assigned user roles define privileges. During the enrollment process, each user has a particular system role or set of system roles to perform using a token. A token is a portable cryptographic universal serial bus (USB) module that provides services that include digital signatures, signature verification, encryption, and decryption.

3-7. Some KMI roles fall under separation of duties considerations for security reasons, as determined by their functions. These external administrative and operational management roles are—

- **Administration roles**—are roles for administration of the client host platform and advanced key processor. These roles consist of the—
  - Client platform administrator.
  - Client platform security officer.
- **Operational management roles**—roles needed to establish and manage the people, products, and equipment associated with a key management infrastructure operating account. These roles consist of—
  - KOAM.
  - Account registration manager.
  - Personnel registration manager.
  - Enrollment manager.
  - Device registration manager.
  - Personnel local type 1 registration authority.
  - Device local type 1 registration authority.
  - CONAUTH.
  - Command authority.
  - Product requester.
  - Key manager.
- **Non-KMI roles** include token security officer.

3-8. External roles fall are either external administrative management or external operational management. External administrative management roles are roles associated with the administration of the client host platform and the advanced key processor. These roles are the client platform administrator and the client platform security officer. External operational management roles are roles needed to establish and manage the people, products, and equipment associated with a key management infrastructure operating account. The client platform security officer requires a KOV-29 token to perform KMI duties, while the client platform administrator does not.

Note. The commander or department head carefully selects individuals to attend the COMSEC account manager and management client courses. Rank, knowledge, skills, abilities, eligibility for retention, and remaining time in Service are part of the selection process.

KEY MANAGEMENT NODES

3-9. The KMI platform provides the hardware, infrastructure, and functionality to support the ordering, generation, storage, establishment, distribution, control, and destruction of cryptographic materials. Customer

organizations may have a mixture of consumers and managers. The KMI consists of three NSA-managed core nodes and the user managed client nodes. The KMI nodes are—

- **Central services node.** Provides a long-term archive of information sent by other system components, and capabilities for analysis.
- **Product source node.** Generates and produces cryptographic keying material based on product or service orders received from the primary services node.
- **Primary services node.** Supports product ordering, management, and distribution while supporting tracking and auditing of system events. Referred to as the KMI storefront.
- **Client node.** Enables customers to access primary services nodes to obtain KMI products and services and to generate, produce, and distribute traditional (symmetric) key products. When configured as the MGC, the client node allows customers to operate locally, and independent of a primary services node. Client node configurations are—
  - MGC node.
  - Client host only node.
  - Delivery only client.

CLIENT NODES

3-10. Client nodes support—

- Operational accounts.
- Operational key management entities.
- Test accounts.
- Test KMI key management entities.
- Schoolhouse and training environment accounts.

MANAGEMENT CLIENT

3-11. The MGC consists of a client host platform that interfaces with the advanced key processor to support cryptographic operations. The MGC enables an external operational manager to manage KMI products and services either by accessing a primary services node when in a client mode configuration or by exercising locally provided capabilities. The MGC supports—

- **KMI enterprise administration**—the MGC supports registration of people, devices, and KMI operating accounts. It supports token issuance and management, user enrollment, and local access to KMI functions and privilege database.
- **Product ordering and management**—the MGC supports the activities of the product manager, CONAUTH, CMDAUTH, and product requester.
- **Product generation and distribution**—the MGC supports the activities required to manage the KMI operating account, its devices, and its agents for local key generation, tracking, and accounting.

TRANSFER KEY ENCRYPTION KEY MANAGEMENT

3-12. A transfer key encryption key (TrKEK) encrypts keys during transfer from the KMI workstation to a fill device; between fill devices and secure telephones; or other NSA-approved over-the-air distribution devices and methods. The receiving secure data system or Simple Key Loader (SKL) uses the TrKEK to decrypt the TEK or key encryption key (KEK) for use in an end cryptographic unit.

***Note*.** All keys downloaded from the advanced key processor in encrypted (black) form; unencrypted (red) output is only authorized to meet a mission-critical requirement.

3-13. Managing and accounting for the TrKEK for encryption and decryption of user keys is at the KMI operating account, except when the local element issues the TrKEK to an end user. The local element manages

and accounts for the TrKEK on an electronic key management worksheet. The KOAM can generate and distribute TrKEKs based on cryptonet or unit design.

3-14. A TrKEK' cryptographic period may be quarterly or yearly. The cryptographic period is quarterly when employing a TrKEK in an extensive network, or transmitting its associated encrypted key by secure means other than the secure telephone or other approved device. The TrKEK cryptographic period is usually yearly for small networks. TrKEKs are classified at the same classification level as the key they encrypt.

FILL DEVICE TRANSFERRING

3-15. Pre-placed TrKEKs reside in the receiving secure data system or SKL. TrKEKs transfer should not take place unencrypted using a secure telephone. The CONAUTH may authorize the production of TrKEKs to a maximum of one year.

3-16. If a remote activity holds at least two secure data systems or SKLs with distinct TrKEKs that expire on different dates, the remote activity does not need to return its secure data system or SKL to the supporting COMSEC account for periodic TrKEK replacement. The supporting COMSEC account may transfer the new TrKEK to remote users' secure data systems or SKLs through over-the-air transfer. The receiving secure data system or SKL can then extract the new TrKEK.

CAUTION

Operators should not attach universal serial bus devices to the secure data system or SKL during red key transfer through the fill port.

FIELD TAMPER RECOVERY CRYPTOGRAPHIC IGNITION KEY AND SUPPORTED NETWORK ENCRYPTION DEVICE

3-17. The field tamper recovery cryptographic ignition key (CIK) provides system administrators the capability to recover a cryptographic device from benign tamper condition. The KOAM is responsible for the accountability and control of field tamper recovery CIKs associated with their account. Field tamper recovery CIKs are accountable in the CMCS as ALC 1 equipment. Field tamper recovery CIKs store and ship separately from associated cryptographic devices, except when in use for tamper recovery.

3-18. When the tamper recoveries on the CIK are exhausted, the equipment is no longer user-recoverable. Accounts turn in non-recoverable equipment and the field tamper recovery CIK to the nearest authorized repair facility for repair or tamper recovery. Units should maintain sufficient backup systems to satisfy mission requirements when equipment becomes inoperable or non-recoverable. The authorized repair facility and property book officer can assist in the replacement of equipment. Depending on the circumstances, the KOAM or maintenance facility may need to initiate COMSEC incident reporting or investigation. Property book officers turn in controlled cryptographic items through normal installation supply channels for depot maintenance.

KEY MANAGEMENT LEVELS

3-19. A multi-tiered key management system enables key management personnel to manage cryptographic keying material throughout the Services. Each management level performs specific functions and duties.

CENTRAL FACILITY

3-20. Central facilities at Fort Meade and Finksburg, Maryland generate all types of keys currently used in U.S. cryptographic systems. Central facilities are also known as KMI storefronts or product source nodes. The central facility produces electronic keys and distributes them through bulk-encrypted transactions.

3-21. Central facilities act as the central office of record for non-military accounts not serviced by a central office of record and as the registration authority for accounts operated by the NSA, contractors, or civilian

entities. The central facility at Finksburg produces and distributes secure data network system key and message signature key. The central facility at Finksburg performs asymmetric seed key conversion and rekey, supports compromise recovery functions, and runs the KMI help desk.

CENTRAL OFFICE OF RECORD—KEY MANAGEMENT INFRASTRUCTURE STOREFRONT

3-22. The central office of record provides oversight and enforcement of Army policies and approved procedures. The central office of record maintains a record of all assigned accountable material and performs regular inventories. The central office of record is also known as the primary services node.

3-23. The KMI storefront allows account managers and user representatives to order the keys necessary to operate their cryptonets. The KMI storefront transfers the keys to KMI accounts electronically and maintains a centralized repository of account registration data with each account's mailing, message, and defense courier addresses, and physical location.

3-24. The central offices of record at Fort Huachuca, AZ and Joint Base San Antonio-Lackland, Texas generate and distribute electronic keys. They also serve as the registration authority, privilege manager, central office of record, and data repository for COMSEC accounts.

KEY MANAGEMENT INFRASTRUCTURE OPERATING ACCOUNT

3-25. KMI operating accounts exchange information directly with their respective central office of record. The KMI accounts at all command levels use the MGC for local real-time electronic key generation, distribution, and management.

3-26. All accounts use the MGC workstation, advanced key processor, secure telephone, a key generator, and an SKL or other electronic fill device to manage electronic keying material. Depending on mission requirements, the COMSEC account may or may not have its own ACES workstation.

3-27. The SKL securely receives, stores, and transfers electronic keys between compatible cryptographic and communications equipment. The SKL integrates the functions of—

- Key management.
- Distribution.
- Electronic protection management.
- SOI management.
- Benign fill.

Automated Communications Engineering Software

3-28. The ACES workstation automates generation, distribution, printing, and storage of cryptonet plans, SOIs, and electronic protection data. It also enables encrypted key distribution and COMSEC key tags for combat net radios.

3-29. The ACES workstation provides general-purpose cryptonet planning, encrypted key distribution, and system-specific key management and distribution. The workstation provides an audit trail, which includes graphic stoplight status indicators.

Management Client

3-30. The MGC electronically manages COMSEC material and provides local key generation and distribution capabilities. The MGC enables management of KMI products and services, either by accessing a primary services node, or through locally provided capabilities.

Management Client Components

3-31. The MGC consists of—

- A personal computer accounted for in the CMCS.
- KMI software, classified at the secret level and categorized ALC 2.

- Client Host Platform hard drives, classified at the secret level and categorized ALC 1. These hard drives are accountable by serial number.
- Advanced key processor, a secret COMSEC device accountable to the central office of record in the CMCS as ALC 1.
- High assurance internet protocol encryptor.
- Bar code scanner.
- Advanced key processor reinitialization drives.
- Advanced key processor CIK.
- Keyboard, monitor, printer, and mouse.
- Type 1 token.
- Advanced key processor adapter.

3-32. The MGC interfaces with the advanced key processor assigned to distribute keys. Figure 3-1 shows components of the MGC.

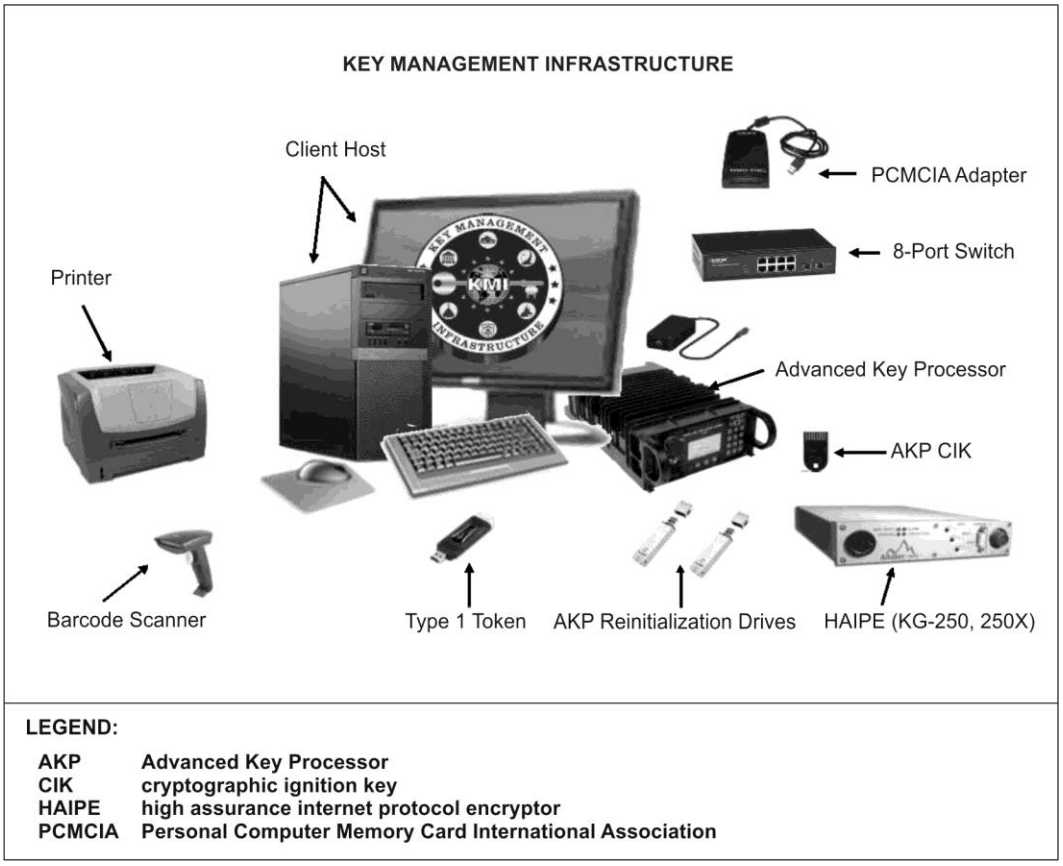

Figure 3-1. Management client components

Management Client Maintenance

3-33. When any part of the MGC node malfunctions, the KMI manager contacts the Department, Agency, Service, or command help desk for assistance. If the help desk cannot resolve the malfunction, the KMI manager follows Department, Agency, Service, or command-directed procedures.

3-34. While the client host platform is under warranty for factory defects, an organization follows warranty guidelines for repair. Upon warranty expiration, the hardware and all associated maintenance is the responsibility of the organization. The organization is responsible for repairs if the hardware becomes non-operational for reasons other than factory defects. Personnel who have at least a secret clearance and work in

a facility authorized to repair computers classified at the secret level perform any maintenance requiring the opening of the client host platform.

Client Host Only

3-35. The client host only is a KMI client without the advanced key processor. The client host only allows command and controlling authorities to access KMI services. The client host only supports product ordering and management, inventory management, and encrypted key downloading. The client host only does not encrypt, decrypt, or locally generate keys, and does not communicate directly with another KMI client node.

Advanced Key Processor

3-36. The advanced key processor is a classified device and trusted component of KMI operating accounts that performs all required cryptographic processing and access control for the KMI account. Advanced key processor functions include—

- Ordering COMSEC material.
- Accounting functions.
- Generating traditional electronic keys.
- Encryption and decryption of asymmetric electronic keys transferred among local elements.
- Encryption and decryption of electronic keys stored in the device database.
- The issue of electronic keys.

3-37. The recertification period of the advanced key processor is seven years from the date of certification. The label attached to the front of the key processor displays the certification date. The account manager contacts the item manager to request a new key processor before the certification date. Once the account is operational with the new advanced key processor, the old device goes back to Tobyhanna Army Depot for recertification. The KOAM contacts the item manager at the CSLA before taking any action. The account needs to stay configured until replacement equipment arrives. These controlled cryptographic items are accountable within the CMCS-assigned ALC 1, tracked by serial number.

3-38. When integrated with the MGC, the advanced key processor receives commands, data, validates the integrity of received commands, and returns data to the workstation. The advanced key processor creates, stores, and outputs an audit trail of its processing activity to the MGC. The advanced key processor has a zeroization feature that allows the operator to delete all classified information in an emergency. Tampering, such as removing the cover, automatically zeroizes the advanced key processor.

LOCAL ELEMENTS

3-39. The lowest level of the KMI architecture consists of local elements. Local elements use fill devices to interface with the COMSEC account and end users they support. Local elements use cryptographic devices to pass key, audit data, key variables, and other required COMSEC files. Local elements receive keying material from the KMI operating account in electronic form using a fill device.

3-40. The Army uses electronic key generation and distribution as its primary means. End users protect and account for all COMSEC material in their possession and report anything that could jeopardize its security or integrity. The unit SOP provides local procedures for safeguarding and controlling COMSEC material. Figure 3-2 on page 3-8 depicts the KMI architecture and levels of COMSEC management.

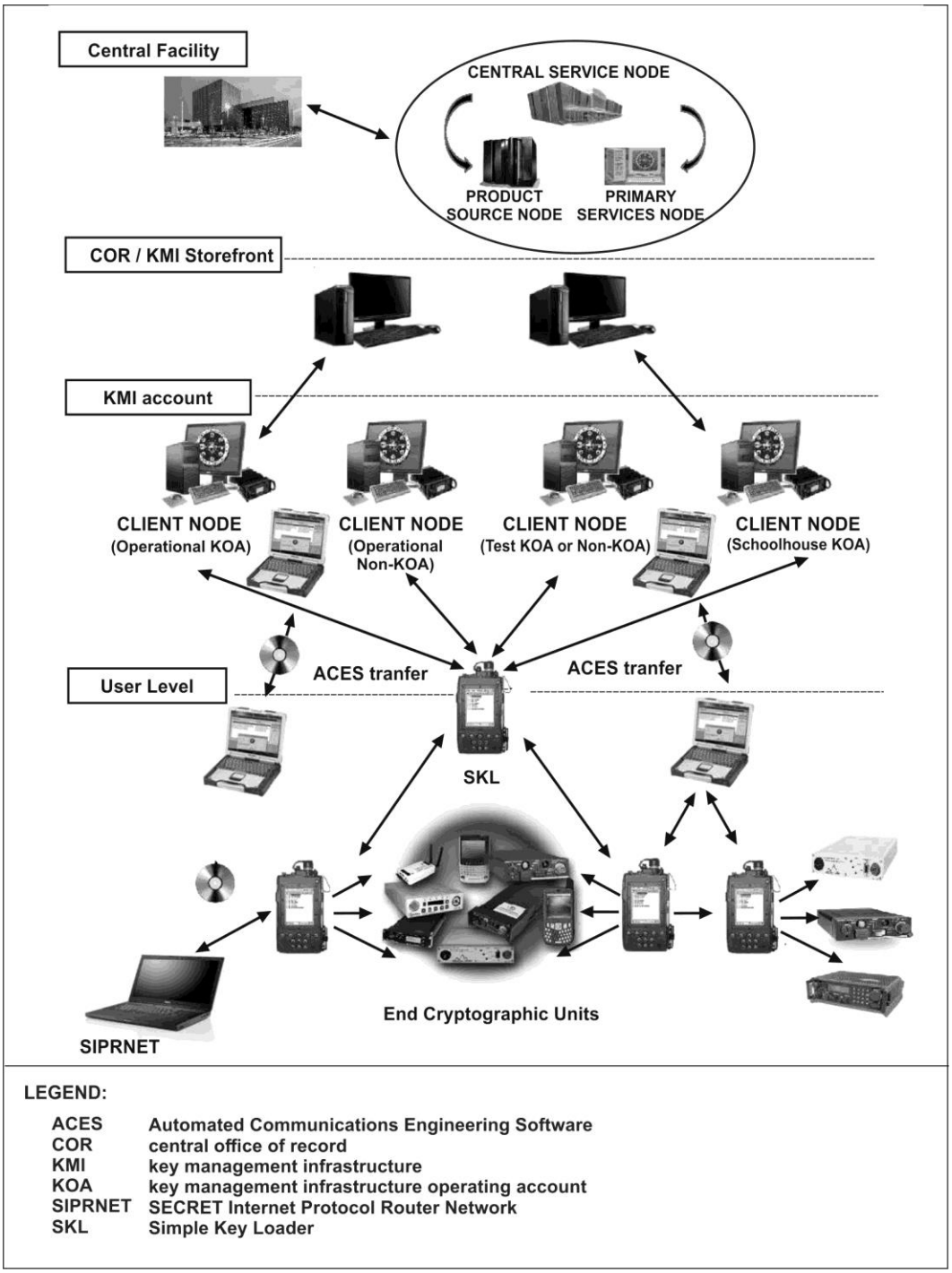

Figure 3-2. Key management infrastructure architecture

KEY TYPES

3-41. Cryptographic keys fall under two general types—asymmetric and traditional. The distribution, implementation, accounting, and destruction requirements vary based on the type of key.

Asymmetric Key

3-42. Asymmetric key implements public key cryptography. Public key cryptography establishes a session key between a public key and a corresponding private key for encryption and decryption. The central facility generates and produces asymmetric electronic keys. Asymmetric keying material has a different supporting structure, including CMDAUTHs and user representatives with functions and responsibilities different from those of CONAUTHs. Asymmetric keys used in the KMI are—

- **Message signature key**—cryptographic material used in the electronic signature process to assure source authentication, message integrity, and non-repudiation.
- **Secure data network system key**—an asymmetric key that does not include the public key infrastructure and is a set of variables used in a key exchange algorithm to produce a TEK.

Traditional Key

3-43. Traditional, key uses the same key variable at both ends of a communications circuit for encryption and decryption. All members of a cryptonet use the same key. Traditional keying material secures sensitive unclassified and classified information. Traditional keys are—

- Symmetric key—both ends of a link or all parties in a cryptonet use the same key.
- High assurance internet protocol encryptor pre-placed and authenticated pre-placed.

Test Key

3-44. *Test key* is key intended for testing of communications security equipment or systems. If intended for off-the-air, in-shop use, such key is called maintenance key (CNSSI 4005). The test key classification level is assigned based on network circuitry or the sensitivity of the information and equipment protected. Test keys may not be used to protect sensitive or classified real-world information. All electronic keys carry the CRYPTO caveat, regardless of generation origin. Use of the test key during training prepares units for real-world operations. Test key requests should list the type of keying material needed and equipment to be protected.

Operational and Seed Key

3-45. *Operational key* is key intended for over-the-air protection of operational information or the production or secure electrical transmission of key streams (CNSSI 4009). Operational key is classified at the same level as the data it protects. The commander and the KOAM determine key requirements based on the unit's mission.

3-46. *Seed key* is initial key to start an updating or key generation process (CNSSI 4009). Operators use seed keys to communicate with the central facility to receive an operational key. The seed key requires the user to perform an initial electronic rekey on the end cryptographic unit. Use of a seed key is the most secure, and therefore the preferred method for key delivery.

KEY GENERATION AND LOCAL GENERATION

3-47. Key generation is the process that creates the first instance of a key. A standard key order contains all mission system independent or dependent data for the destination COMSEC equipment to generate the correct key. Electronic key generation can occur at the central facility, central office of record, or at the KMI account. When commanders direct a KOAM to generate a local key, the command and staff become the CONAUTH for that key and assume responsibility to provide all services to net members using the cryptonet and key.

3-48. KMI workstations can produce traditional electronic keys, such as a TrKEK, KEK, or TEK. Account managers register or generate appropriate privileges before generating these keys. The MGC and advanced key processor give this workstation the capability to generate keys and produce new short titles, if not already assigned. Each item of accountable COMSEC material is assigned a short title to facilitate handling, accounting, and control.

FILL DEVICES

3-49. Fill devices read, transfer, and store keys. Currently fielded fill devices provide an audit trail of all key actions and transactions. The MGC can upload audit data from, and send encrypted key and application data to, a fill device.

CRYPTOGRAPHIC IGNITION KEY

3-50. The advanced key processor uses a CIK to unlock its secure mode. The key processor has a CIK interface, USB port, and a fill port. Only an authorized operator with a valid CIK can use the key processor. Unencrypted and encrypted COMSEC distribution takes place through the key processor's fill device interface or USB interface. Each key processor has a minimum of two CIKs. The primary user can procure additional CIKs as necessary.

Chapter 4
Key Distribution

This chapter discusses distribution planning, over-the-air distribution, encrypted key distribution, and the Defense Courier Division. This chapter further discusses communications security considerations for joint and multinational operations and the deployment of COMSEC support.

DISTRIBUTION PLANNING

4-1. Key distribution is the secure, accountable process of moving the key from the point of generation to the point of use. Electronic distribution included the necessary packaging, copying, reformatting, encryption, and relaying requirements to transfer the key from its origin to the point of use. When possible, keys remain encrypted until loading into the end user equipment.

4-2. The CMDAUTH or CONAUTH designates the explicit intent for local key generation, in writing. The KOAM oversees key distribution for users according to COMSEC policy and procedures. The KOAM may distribute keys if there is a valid distribution authorization on file from the CONAUTH. The commander or CONAUTH identifies the key for special handling, control, and restricted distribution based on its intended use and the information or network it protects. COMSEC distribution takes place through—

- **Transfer**—the distribution of COMSEC material from one account to another. Transfers move accountability and responsibility for the transferred COMSEC material from the sending account to the receiving account.
- **Issue**—the distribution of one or more accountable COMSEC items from a COMSEC account to a local element. The issuing element retains accountability for the material. Issuing and filling keys are the two functional areas of key distribution between a KMI operating account and a local element.

4-3. The MGC issue function is the local accountability of one or more accountable items from a KMI operating account to a local element. The account distribution profile stores the information needed to issue keys. The profile stores the list of keys, eliminating the need to routinely enter the same requests for issue. The issue function contains most of the processing needed to prepare keying material for end users. The issue function removes a key from local storage, maps the key to its end cryptographic unit, and prepares the key for acceptance, transmission, and loading into the end cryptographic unit.

4-4. The filling function loads the key into an end cryptographic unit. Refer to equipment technical manuals for loading instructions for specific end cryptographic units.

KEY DISTRIBUTION METHODS

4-5. The method used to distribute keys depends on the medium used for distribution and the sending and receiving local element capabilities. Key transfers may take place using optical media, a fill device, or telecommunications channels. The medium used to transfer keys depends on the current storage medium of the key.

4-6. The net control station may initiate over-the-air key distribution any time during the effective cryptographic period, or immediately before the end of the cryptographic period. Before transmitting a key, the net control station notifies all recipients over a secure communications link and outlines the details of key transmission. Notification includes—

- Time of the key transmission.
- The identity of the circuit and key.

- Destination instructions for recipients.
- Short title, classification, effective period, and CONAUTH of the key.

4-7. Users that receive a key from sources other than the MGC acknowledge receipt of the key by signing local custody documents. Custody documents record—

- Short title or designator.
- Classification.
- Date of generation and loading.
- Date of issue or transfer.
- The identity of issuer and recipient.
- CONAUTH of the key.
- The effective period of key.

KEY WRAPPING AND DISTRIBUTION TECHNIQUES

4-8. The National Advisory Group Publication NAG-16F is the standard user manual for planning and performing electronic key generation, over-the-air rekeying, and over-the-air transfer. NAG-16F provides detailed instructions for—

- Over-the-air rekeying and over-the-air transfer procedures using the fill device.
- Allied over-the-air rekeying.
- Use of inter-theater COMSEC package generic key as over-the-air rekeying and over-the-air TrKEK.
- Procedures for distributing keying material through the Defense Switched Network, general service message system, or secure telephone.
- Unsuccessful over-the-air rekeying.
- Late entry or reentry to networks.
- List of approved 128-bit cryptographic-equipment.
- Procedures for transferring keys between fill devices using a secure telephone.

OVER-THE-AIR KEY DISTRIBUTION

4-9. Over-the-air key distribution reduces the need to transfer keying material physically, by allowing secure transfer of keys and files over a secure communications network. Over-the-air distribution methods are—

- Over-the-air rekey.
- Over-the-air transfer.
- Over-the-network keying.

OVER-THE-AIR REKEYING

4-10. Over-the-air rekeying is a method of updating cryptographic keys over the communications networks they secure. Over-the-air rekeying changes the TEK or the TSK in remote cryptographic equipment by sending a new key.

4-11. The variable generate option on the SKL generates a key that can be sent to a user to produce a TEK. The over-the-air distribution option allows the operator to generate a key and store it in the SKL for later distribution to an end cryptographic unit. The CONAUTH authorizes the use of the variable generated.

4-12. The variable update option provides the ability to send a KEK to a device with variable update capabilities to perform a deterministic key update and return the revised key to the SKL. The SKL retains both the original and updated KEKs. The original tag applies to the updated KEK. The segment number and suffix fields increment by one.

4-13. The manual rekey option allows a net control station to send a TEK to the network members. The net control station contacts the network members, and the network members prepare their equipment for receiving

a TEK. The net control station informs network members how and when to switch the key. Requirements for manual rekey include—

- Net control station KEK short title and text identity.
- Outstation KEK short title and text identity.
- Channel of the outstation's radio on which the TEK is stored.
- New or replacement TEK short title and key attributes.
- Review of all procedural steps before performing a manual rekey operation.

OVER-THE-AIR TRANSFER

4-14. Over-the-air transfer electronically distributes a key without changing the TEK used on the secured communications path. The SKL can connect to a variety of secure devices through a secure communications path. The preferred method to transfer keys is through an SKL database transfer. If the sender does not do a database transfer, the receiver must manually input the effective dates, cryptographic period, and supersession date. Manually entering these parameters requires care to prevent operator error. Figure 4-1 depicts over-the-air transfer options.

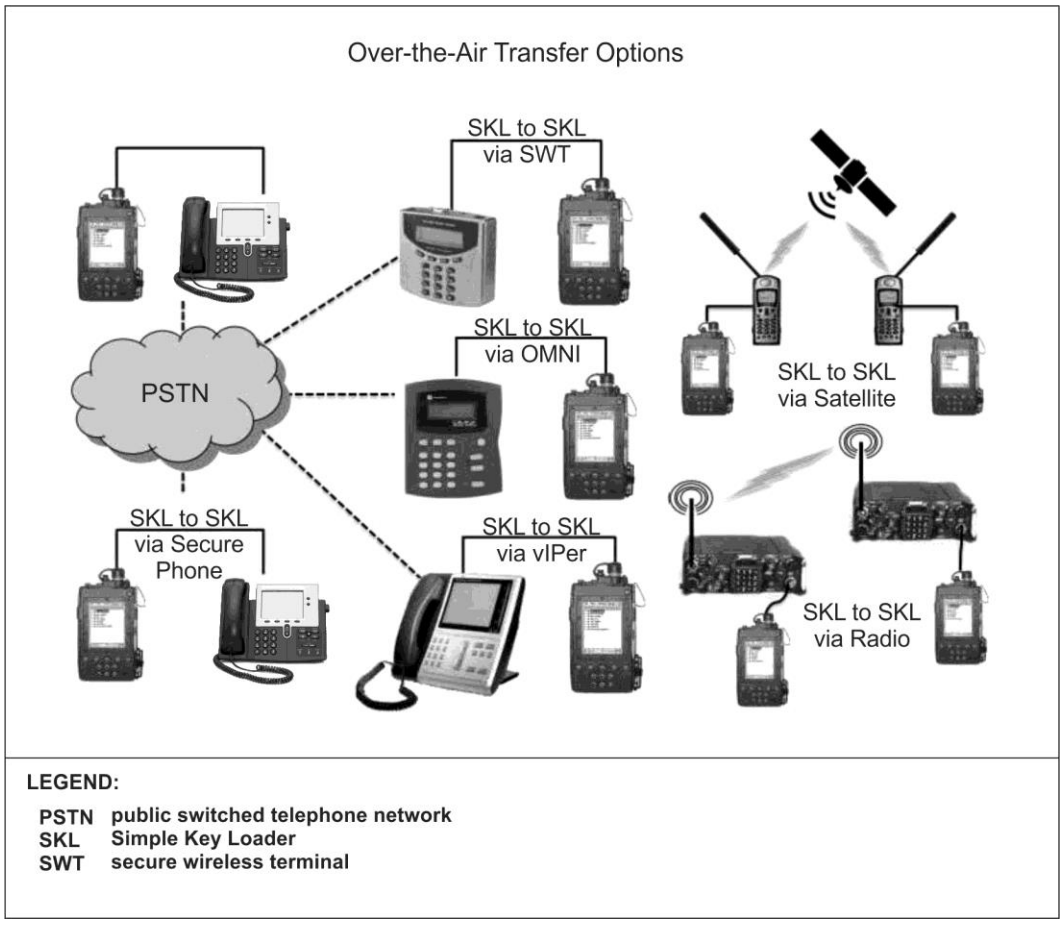

Figure 4-1. Over-the-air transfer options

Note. The secure wireless terminal and OMNI are scheduled for removal from the Army inventory by 2021.

OVER-THE-NETWORK KEYING

4-15. Over-the-network keying enables a device to receive electronic COMSEC keys directly from the primary services node (KMI storefront) or an MGC. Over-the-network keying prevents the need to physically deliver COMSEC keys to net members in high-risk or remote locations. Over-the-network keying saves time versus physical distribution of keys and reduces risk to the unit and mission.

ENCRYPTED KEY DISTRIBUTION

4-16. Figure 4-2 depicts encrypted key distribution, which is the process of electronically issuing COMSEC keys over the SECRET Internet Protocol Router Network (SIPRNET). Encrypted key distribution uses a locally generated TrKEK to secure the key transfer. Encrypted key distribution allows secure delivery of a key to an end cryptographic unit and reduces the risk of compromise during transmission.

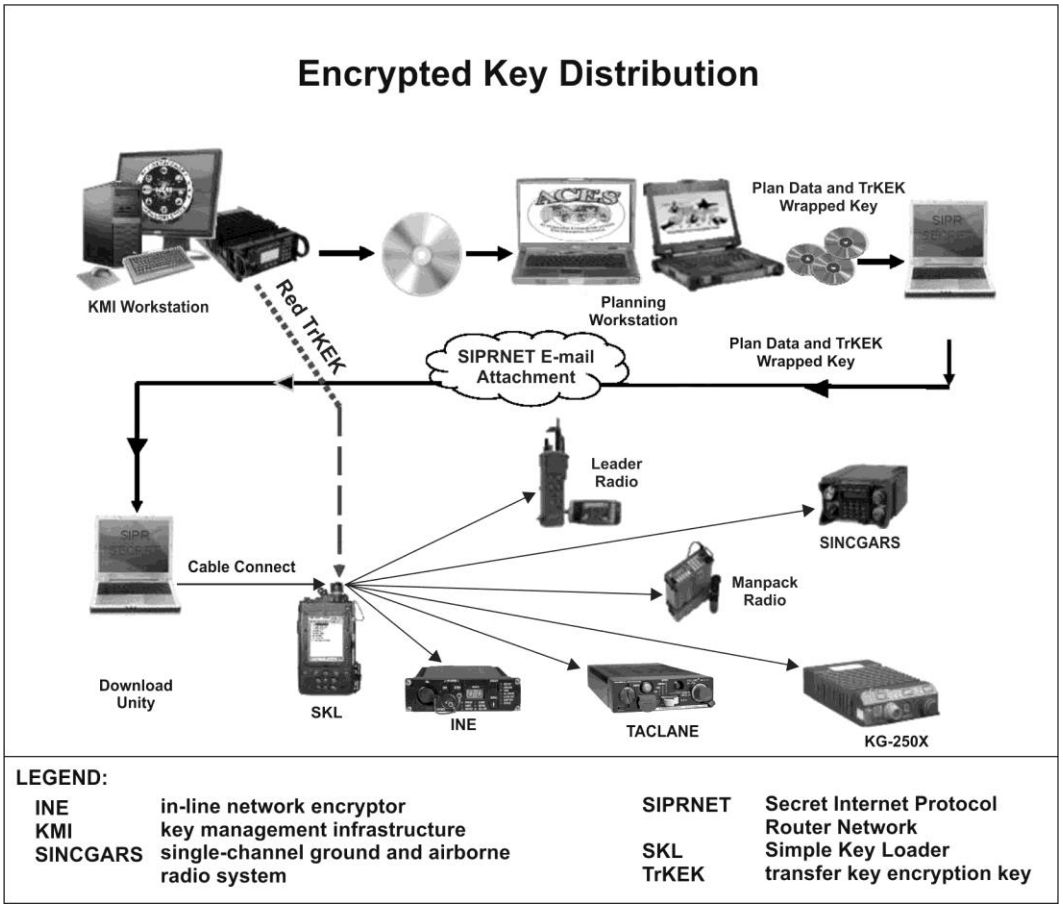

Figure 4-2. Encrypted key distribution chart

4-17. Encrypted key distribution starts with the KOAM using the planning workstation to generate an encrypted key. The download utility software downloads the key and data file to a radio set or other end cryptographic unit. This file, along with the magnetic media or device, is classified secret and accounted for and destroyed in accordance with regulations and local policy.

4-18. The baseline software and hardware requirements for encrypted key distribution are—

- **MGC**. Dedicated to KMI and capable of performing many functions independently of a primary services node. The MGC provides cryptographic processing using the advanced key processor.
- **ACES**. Automates secure cryptonet planning and distribution of COMSEC materials, including key tagging information, electronic warfare materials and SOIs. Implementation of encrypted key requires the current software version.

- **Common User Application Software**. Resides on the MGC workstation to facilitate creating and loading encrypted keys to removable media.
- **SKL**. Receives stores, manages, and distributes electronic keys for loading into end cryptographic units. The SKL provides mission data (hop-sets, loadsets and SOI information) distribution and loading for various systems.

COORDINATION

4-19. COMSEC managers coordinate with and obtain assistance from personnel performing encrypted key distribution. G-6 (S-6) staffs coordinate with spectrum managers to use the ACES terminal for key distribution. Encrypted key distribution requires SIPRNET access at both the transmitting and receiving ends.

AUTOMATED COMMUNICATIONS ENGINEERING SOFTWARE WORKSTATION

4-20. The ACES workstation can import encrypted keys from the MGC. Encrypted key handling allows secure key distribution between ACES workstations and downloading to fill devices. The workstation provides the capability to issue encrypted keying material in an end cryptographic unit KEK for distribution on optical media. The ACES workstation can import and further process encrypted key packages from optical storage media. The encrypted key packaging capability available on the MGC and common user application software, with the capability incorporated in ACES, satisfies the encrypted key handling requirement for identification, friend or foe mode 5.

ENCRYPTED KEY PACKAGING

4-21. Encrypted key packaging starts with the receipt and identification of the red key from the NSA central facility. Distribution from the central facility to each COMSEC account requiring a specific key occurs on scheduled distribution timelines. At the unit level, COMSEC planners determine the best method for distributing keys. Depending on the deployment requirements, this may involve distributing a single encrypted key package to one ACES workstation or multiple packages to multiple ACES workstations. Some circumstances require the distribution of only a limited quantity of future keys.

4-22. The MGC workstation operator generates a red key using the symmetric key option. The symmetric key serves as the end cryptographic unit KEK.

4-23. The COMSEC planner uses Common User Application Software to encrypt keys for distribution using the red symmetric key. Using the local element issue setup procedure, workstation operators routinely issue encrypted electronic keys on optical media. The COMSEC planner selects the keys to encrypt, selects the red KEK for encryption, and distributes the encrypted key package on optical media. Local users load the encrypted key—wrapped in the symmetric key—into the end cryptographic unit. The ACES workstation operator imports encrypted keys from optical media and transfers them to a fill device for distribution and loading into end cryptographic units.

DISTRIBUTION TO END CRYPTOGRAPHIC UNITS

4-24. COMSEC planners make provisions to distribute red KEK to each end cryptographic unit. The only method approved to distribute red KEK is the use of an SKL. For identification, friend or foe mode 5, the same SKL may handle distribution of both the red KEK and the encrypted key. The network planner uses the SKL containing the red KEK to download the encrypted key and further distribute keys to end cryptographic units.

4-25. Common user application software provides the ability to deliver encrypted key packages to local users' fill devices. Encrypted key enables secure distribution of a relatively large volume of key between U.S. forces and allies.

4-26. Operators may distribute the red KEK separately to the end cryptographic units. Once the red KEK is distributed and loaded, the end cryptographic unit can unwrap the encrypted key. An encrypted key may contain classified or sensitive unclassified attributes, such as its associated header or tagging information. This data may be either encrypted or unencrypted. If the data is unencrypted, the entire data package assumes the classification of the header data.

PROCESS

4-27. Encrypted key distribution delivers electronic keys over SIPRNET using the MGC and ACES. The supporting COMSEC account wraps keys with their TrKEK. The TrKEK encrypts keying material for transportation between KMI operating accounts and end user devices.

4-28. A TrKEK is unique to the COMSEC account that generated it. Only users with the same TrKEK can access the keying material from that account. The use of TrKEKs prevents adversaries or unauthorized users gaining access to keying material or the cryptonets it secures. A primary or alternate KOAM or other authorized person loads the fill device with the TrKEK before loading the encrypted key package.

4-29. The COMSEC planner wraps keys with a TrKEK using Common User Application Software. The Common User Application Software produces an encrypted key package that gets written to removable storage media. The process writes two files to the storage media. The identify.txt file identifies the local element it is going to, short title, edition, and the register number of the encrypted key package. The KEYSET.xml file contains the encrypted key. The COMSEC account imports files from the storage media to the ACES workstation by uploading the .xml file. The operator uses the tier 3 download tool to change the .xml file to a .bin format. The planner can then download the file to removable storage media for transfer to a SIPRNET workstation. The planner uses SIPRNET e-mail to transfer the file to the customer. The local element uses the tier 3 download application on their SIPRNET workstation to load the file to a fill device.

4-30. An SF 153 (*COMSEC Material Report*) or an electronic key management worksheet documents accountability of keying material. Once the customer receives the encrypted key package, the local element signs and returns the hand receipt documents to the KOAM. These files remain on the customer's e-mail and workstation. Therefore, detailed destruction procedures need to be in place for the encrypted key package when sent by SIPRNET.

Note. The electronic key management worksheet is available in TB 380-41.

TRANSMISSION OF ENCRYPTED KEYS

4-31. Distribution of encrypted keys, encrypted software, or other encrypted data should take place over networks certified to process U.S. secret or higher classification. Unclassified or multinational networks should not be used to send these keys and encrypted data. An encrypted key is considered non-cryptographic until it is decrypted. After receiving and decrypting a data package containing encrypted keying material, the original encrypted data package requires no further accounting.

4-32. Decrypted keys become cryptographic, and require safeguarding, control, and accounting according to the procedures for red keys. Unencrypted keying material intended to encrypt operational data remains cryptographic and is accountable in the CMCS. Decrypted keys are also accountable in the CMCS. Keys decrypted in a machine from which unencrypted key cannot be extracted, such as benign fill equipment, do not require additional accounting.

DESTRUCTION OF ENCRYPTED KEYS

4-33. The COMSEC SOP should address proper accountability and destruction procedures for removable media. Users should zeroize the KEK as soon as practical after supersession. Users can destroy encrypted electronic key and its associated KEK by zeroizing all copies of the KEK. Zeroization overwrites the key.

4-34. COMSEC personnel must destroy all unencrypted (red) copies of electronic keys within 12 hours after supersession. Storage media that has previously held cryptographic keying material is reusable, but it retains the highest classification of any key previously held.

DEFENSE COURIER DIVISION

4-35. The United States Transportation Command Defense Courier Division provides secure, timely, and efficient end-to-end global distribution of classified and sensitive material for the United States and its allies. Each courier station provides courier service to customers within a defined geographic region. Courier stations

distribute COMSEC material through regularly scheduled Defense Courier Division missions. The United States Transportation Command director of operations approves requests for special movements to transport or ship COMSEC material before mission execution.

LEVELS OF SERVICE

4-36. Classified and sensitive unclassified materials are eligible for shipment by the Defense Courier Division, according to two levels of service—

- **Regular shipment** represents the bulk of the material transported by defense courier. This material ships through regularly scheduled missions. The majority of COMSEC material transports takes place through regular shipment.
- **Special shipment** is expedited transport at the expense of the requesting command when regularly scheduled missions cannot satisfy deadlines. The Defense Courier Division may require the requesting customer meet with the courier at a pre-coordinated site.

MATERIAL QUALIFIED FOR SHIPMENT

4-37. DODI 5200.33 defines qualified and prohibited material for Defense Courier Division shipment. Any sensitive material requiring courier escort is qualified for movement by the Defense Courier Division. Examples of qualified material include—

- Top secret information.
- Classified material, including cryptographic and COMSEC material.
- Classified cryptologic material.
- Cryptographic keying material designated and marked CRYPTO by the NSA.
- Sensitive compartmented information.
- Aerial and satellite imagery classified secret or higher.
- Controlled cryptographic or COMSEC items, and other cybersecurity products or materials identified by the NSA as requiring courier service.
- Nuclear command and control materials.
- Secret collateral material for the intelligence community.
- Technical surveillance countermeasures material.
- Diplomatic courier pouches.
- Any other classified material.

PROHIBITED MATERIAL

4-38. Materials prohibited from movement by Defense Courier Division regardless of security classification include—

- Contraband, including controlled substances.
- Personal property.
- Explosives, ammunition, firearms, and their components.
- Radioactive, etiological (disease-causing), or other materials hazardous to humans.
- Perishable materials that require refrigeration or icing.
- Hazardous materials.
- Liquids of any kind.
- Batteries regulated as hazardous materials.
- Currency, military payment certificates, bonds, securities, precious metals, jewels, postage stamps, or other negotiable instruments.

JOINT AND MULTINATIONAL OPERATIONS

4-39. The joint force commander may direct establishment of a joint COMSEC management office to provide long-term COMSEC material support in the joint operations area. The joint COMSEC management

office consists of personnel from all Services. The structure is not fixed; it may be task organized in any combination. The joint COMSEC management office provides a forward-deployed COMSEC office. The joint COMSEC management office stores, maintains, distributes, destroys, issues, processes, and transports COMSEC materials into and within the joint operations area. Each unit commander should be prepared to initiate and execute agreements with the joint and Army theater COMSEC management offices, or other Services' COMSEC management offices to ensure availability of keying material needed to support their operations.

4-40. North Atlantic Treaty Organization and other multinational operations require communications interoperability. The servicing COMSEC management office provides policy and procedural guidance for releasing COMSEC material and controlled cryptographic items to multinational mission partners. All COMSEC keying material and equipment that require transfer to multinational partners require approval from Headquarters, Department of the Army Deputy Chief of Staff, G-2. Operation orders, SOIs, and related documents identify the cryptosystems required to support joint and multinational operations. Commands establish eligible multinational partners as local elements according to national policy, regulations, and guidelines.

DEPLOYMENT COMMUNICATIONS SECURITY SUPPORT

4-41. Upon notification of a pending deployment or exercise, the commander determines whether the unit will deploy with or without its COMSEC account. When an existing COMSEC account can adequately support its COMSEC requirements in the deployment area of operations, the unit may leave its account behind in the care of another account. Unneeded COMSEC equipment can be stored at a secure facility.

4-42. If the commander decides to store COMSEC equipment at a secured facility, the commander suspends the account until the unit returns to the home station. The commander may also opt to leave the account active with the KOAM not deploying and continuing day-to-day operations at home station. The commander's decision whether to deploy with the COMSEC account should consider—

- Availability of COMSEC support in the deployment area.
- Forces requiring COMSEC support—
  - Army.
  - Joint.
  - Multinational.
  - Inter-organizational partners.
- COMSEC requirements at the deployment location and at home station.
- Length of deployment.
- The requirement to support other units at the deployment locations.
- Communications connectivity to the central office of record and KMI storefront.
- Accessibility of the supporting unit's COMSEC account.
- Type of COMSEC material required for operations.
- Systems, circuits, and types of secure communications required at the deployment location.
- Mission change while deployed.

4-43. The account manager assists the commander in finalizing deployment plans. The commander of the deploying unit should—

- Coordinate with the theater army G-2 and operations staff section.
- Coordinate with the gaining combatant command intelligence and operations staff.

4-44. If the unit ships COMSEC material to the deployment area, the KOAM prepares the material for shipment in accordance with AR 380-40. Refer to TB 380-41 for detailed procedures for moving COMSEC accounts.

4-45. Units deploying with their COMSEC accounts should contact the theater COMSEC office in the deployment theater. The theater COMSEC office provides oversight for all theater accounts, issues keying material to deploying accounts, processes key ordering requests, and receives reports of keying material

disposition from accounts in theater. The theater COMSEC office assists account managers with Defense Courier Division shipments. The theater COMSEC office receives equipment and COMSEC keying material for deployed accounts and serves as the central distribution point for replacement of MGCs and key processors. Account managers should consider suspending scheduled delivery of keying material not needed in the theater until shortly before they redeploy to home station. This eliminates the need to account for, store, and destroy unneeded COMSEC material.

This page intentionally left blank.

Chapter 5
Accounting

This chapter addresses communications security material accounting, including certificate management, hand receipts, compromise recovery, incident evaluation and types, maintenance, and two-person integrity for top secret communications security materials.

CERTIFICATE MANAGEMENT

5-1. Certificate management is a process for generating, storing, protecting, transferring, loading, using, and destroying certificates. Each KMI account uses an asymmetric key that cryptographically identifies the element by its KMI identification. The asymmetric key is valid for one year from generation. Operators electronically rekey the set each year to remain valid. The rekeying process allows the KOAM to transfer keys between COMSEC accounts. This creates public and private keys to protect transfers. These credentials are valid for one month. Users can create up to 12 credentials.

5-2. The CONAUTH posts the credentials to the KMI directory service. When a user account needs to transfer keying material to another element, they connect to the directory service to download the distant end's public key and account information. The local key processor uses the distant end's current public key to encrypt the keying material. This process produces a bulk-encrypted transaction. Decryption takes place at the distant end using the private key.

HAND RECEIPTING COMMUNICATIONS SECURITY MATERIAL

5-3. The issuance of COMSEC material on a hand receipt transfers and delegates responsibility for the material to the receiving individual. Accountable items include symmetric and asymmetric key, classified or CMCS controlled COMSEC equipment, and COMSEC aids, along with operating and maintenance manuals. Accountable COMSEC material is not hand receipted between COMSEC accounts but may be hand receipted to individuals including other KOAMs.

5-4. Before releasing or approving the release of COMSEC material, the KOAM verifies the recipient's security clearance, availability of approved storage and operation facilities, and need to know, based on formal documentation. The KMI workstation creates and maintains records of accountable items and manipulates and modifies data contained in these records.

ISSUE OF KEYS TO A LOCAL ELEMENT

5-5. The commander or designated representative may appoint an individual as a COMSEC local element, provided the individual has a valid need for the material. The local element must be a U.S. citizen with the necessary security clearance and the facilities to properly secure the material. This includes government contractors providing services to U.S. forces, whether in the continental United States or at overseas installations. In the absence of the KOAM, alternate KOAMs require prior approval from the commander or equivalent to issue COMSEC material to individuals not already authorized as a local element.

Note. The hand receipting of COMSEC material from a KOAM to a local element transfers and delegates responsibility for the COMSEC material to the local element. The KOAM continues to account for that material to the central office of record. The KOAM accounts for COMSEC material as hand receipted until it is turned in or otherwise disposed of with proper documentation.

5-6. An SF 153 accompanies COMSEC material issued to a local element. The material may remain on a hand receipt for up to two years. Every two years, the KOAM generates new hand receipts for the local element to sign. When a local element receives COMSEC material, they assume full responsibility for safeguarding it. Account managers may use other forms in place of an SF 153 under unusual or emergency conditions, if the form used contains the required hand receipt information.

5-7. The KOAM ensures all local elements receive appropriate training on the safeguarding, destruction, inventory and operating instructions for the material provided. Local elements receive a COMSEC briefing and cryptographic access briefing as required and sign attesting completion of briefing.

5-8. The local element for secret and top secret material must maintain a security clearance equal to or higher than the highest classification level of the material to which the element has access, and be enrolled in the Department of the Army cryptographic access program. Issue of top secret material requires for two local elements, one being a cleared witness. Both local elements sign the SF 153 to document two-person integrity.

5-9. The issuing KOAM keeps the original SF 153. The local element receives a duplicate copy and disposition record DA Form 5941-R (*COMSEC Material Disposition Record*) or electronic key management worksheet for the material used. Before taking possession of COMSEC material, the local receiving element—

- Inventories the material against the system generated SF 153.
- Verifies presence of all pages of unsealed COMSEC material and publications.
- Verifies presence of all electronic keying material received into a fill device.
- Corrects the SF 153, if necessary, and initials all corrections.
- A second authorized individual signs when receiving top secret material from the KOAM, meeting two-person integrity requirements.

5-10. Both the issuing KOAM and the local element maintain files that serve as the record of accountability and responsibility for material issued to the local element. Upon return of the material, or verification of final destruction, the KOAM removes the original SF 153 from the file and returns it to the local element receipt holder. There is not a requirement for the local element to retain a file copy of the original SF 153.

DESTRUCTION OF COMMUNICATIONS SECURITY MATERIAL

5-11. Destruction of accountable COMSEC material requires the presence of a destruction official and a witness. Both individuals must possess a security clearance equal to or higher than the classification of the material they are destroying and both must be present throughout the destruction process. The destruction official and witness properly destroy COMSEC material, prepare a destruction report, and ensure destruction meets the appropriate standards of TB 380-41. The improper destruction of classified or unclassified material is a reportable COMSEC incident and may lead to potential adversaries obtaining sensitive information.

5-12. Account managers should destroy keying material within 12 hours of supersession, after the keying material serves its intended purpose, or according to written CONAUTH and CMDAUTH guidance. This includes superseded COMSEC material hand receipted to a user and the COMSEC account, regardless of location.

DEFECTIVE KEYS AND INCIDENT REPORTING

5-13. COMSEC account personnel and users do not destroy defective or faulty keys. They immediately report defective keys through the Communications Security Incident Management Monitoring System.

5-14. The Communications Security Incident Management Monitoring System is a SIPRNET web-based portal with a data-driven application that allows KOAMs and property book officers to submit incident reports electronically to the Communications Security Incident Monitoring Activity, Army command, Army Service component command or direct reporting unit, CONAUTH, CMDAUTH, and local counterintelligence element. The Communications Security Incident Management Monitoring System prompts the user for the information to complete a COMSEC incident report and has a help feature to assist with navigating the application. The United States Army Communications Security Incident Monitoring Activity notifies the NSA while the KOAM and users await disposition instructions.

5-15. All personnel who possess, handle, operate, maintain, or repair COMSEC material must follow physical security and cryptographic security policies and procedures. Security violations are reportable to the COMSEC facility supervisor, KOAM, and the commander. All persons responsible for protecting COMSEC material must be able to recognize any incident that may develop into a COMSEC insecurity and report it to the appropriate security authorities. Undetected or unreported incidents or compromises are particularly dangerous, since they go unmitigated. Reportable COMSEC incidents include—

- Loss of accountability.
- Improper destruction.
- Possible tampering.
- Failure to perform key processor changeover.
- Found on installation.
- Unsecured or unauthorized access.
- Improper storage of COMSEC material or equipment.
- Unauthorized use of keying material.
- Loss of COMSEC material.
- Loss of two-person integrity.

COMPROMISE RECOVERY

5-16. The CONAUTH must take immediate corrective action to address compromised keys. The CONAUTH should have a plan in place for replacing compromised keying material. The CONAUTH immediately notifies all cryptonet members when a network key is compromised and advises the commander, who determines whether to initiate emergency supersession or extend the cryptographic period of the network key by exception.

EMERGENCY SUPERSESSION

5-17. Where substantial evidence exists of a keying material compromise, the CONAUTH normally announces immediate precautionary supersession and directs early implementation of an uncompromised replacement key. The CONAUTH directs review of any record traffic encrypted using the compromised keying material, when warranted.

EXCEPTIONS

5-18. Superseding an electronic key can present unacceptable risk for mobile or local users, depending on the tactical situation. Geographically separated users who do not have, or cannot receive, the replacement key will lose access to the communications network until they can receive and activate the new key. The commander must weigh the operational risk of immediate supersession.

5-19. When supersession is not feasible or presents an unacceptable operational risk, the commander may direct the CONAUTH to—

- Extend the cryptographic period of uncompromised keying material.
- Exclude net members who do not hold or cannot get replacement material.
- Suspend cryptonet operation until the key can be replaced.
- Continue to use the compromised material when—
  - Normal supersession of compromised material occurs before emergency supersession date.
  - Keying material changes may adversely affect operations.
  - No replacement material is available.

INCIDENT EVALUATION AND INCIDENT TYPES

5-20. CONAUTHs evaluate COMSEC incidents locally. In case of COMSEC material compromise, the CONAUTH informs the United States Army Communications Security Incident Monitoring Activity and the NSA promptly. COMSEC incident reporting requires a SIPRNET token to access the Communications

Security Incident Management Monitoring System portal. Exceptions to this process are if there is an extended network outage or electronic means of reporting are unavailable. If this happens, reporting units can temporarily report the incident manually.

5-21. Incident reporting allows officials to determine whether the incident seriously affected the security of a cryptosystem or has the potential to harm national security. Incident reporting provides the basis for identifying incident trends and for developing policies and procedures to reduce or eliminate similar future incidents.

5-22. AR 380-40 identifies three categories of reportable COMSEC incidents—

- **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.
- **Cryptographic incident**—is equipment malfunction or error by an operator or account manager that adversely affects the cryptographic security of a machine, auto-manual cryptosystem, or manual cryptosystem.
- **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.

5-23. In addition to physical, cryptographic, and personnel security incidents, administrative incidents may occur. An *administrative incident* is a violation of procedures or practices dangerous to security that is not serious enough to jeopardize the integrity of a controlled cryptographic item, but requires corrective action to ensure the violation does not recur or possibly lead to a reportable COMSEC incident (CNSSI 4001). Physical, cryptographic, personnel, and administrative incidents involving cleared personnel require reporting to security managers.

Note. Any unmanned aerial vehicle involved in one or more of the above-listed events constitutes a reportable COMSEC physical incident (see AR 380-40).

MAINTENANCE

5-24. Under the two-level maintenance system, units maintain COMSEC equipment based on maintenance allocation charts in Army technical manuals. The maintenance allocation chart designates which tasks maintainers may perform at each level.

5-25. Field maintenance support organizations perform tasks coded C for operator, crew, and signal support specialist, or F for maintainer. Trained and certified COMSEC maintainers perform serviceability tests, technical inspections, and authorized repairs.

5-26. Maintenance organizations turn in equipment that is not repairable at the field maintenance level to Tobyhanna Army Depot or the nearest forward repair activity for repair or disposal. Tobyhanna Army Depot or the forward repair activity performs sustainment maintenance tasks listed under maintenance tasks code D in the maintenance allocation chart.

5-27. Units turn in unserviceable classified COMSEC material through the CMCS and unclassified COMSEC equipment, including controlled cryptographic items, through supply channels. Refer to ATP 4-33 for more information about COMSEC maintenance.

TWO-PERSON INTEGRITY

5-28. Top secret keying material protects the most sensitive national security information. Its loss to an adversary can compromise all information protected by the key. Foreign intelligence entities consider top secret key as a high priority target for exploitation. For this reason, top secret key requires special protection. Two-person integrity and no-lone zones meet this requirement.

5-29. *Two-person integrity* is the system of storage and handling designed to prohibit individual access to certain COMSEC keying material by requiring the presence of at least two authorized persons, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed (CNSSI 4009) Commanders may assign personnel a two-person integrity-only role if the account does not have three fully-trained account managers. Two of the alternates can be two-person integrity-only if they have not completed the required COMSEC training but possess the required security clearance. Two-person integrity-only account managers serve only as the second person in the absence of the primary or alternate KOAM during top secret transactions. Two-person integrity-only users cannot have Windows log-in accounts to the KMI system.

5-30. No-lone zones are required for access to top secret keying material. A *no-lone zone* is an area, room, or space which, when manned, must be occupied by two or more appropriately cleared individuals who remain in sight of each other (CNSSI 4009). Violations of two-person integrity are reportable COMSEC incidents, as specified in AR 380-40 and TB 380-41.

Note. The commander can modify two-person integrity rules for users operating in hostile fire zones, imminent danger zones, combat zones, and tactical situations.

This page intentionally left blank.

Chapter 6
Controlled Cryptographic Items

This chapter provides an overview of controlled cryptographic items and discusses requirements for accountability, transfer, storage, and release to foreign nationals. This chapter further discusses protective technologies, transfer of controlled cryptographic items between Services or agencies, and maintenance of controlled cryptographic items.

OVERVIEW

6-1. A *controlled cryptographic item* is a secure telecommunications or information system, or associated cryptographic component, that is unclassified and handled through the communications security material control system, an equivalent material control system, or a combination of the two that provides accountability and visibility (CNSSI 4009). Controlled cryptographic items are unclassified COMSEC equipment that contain a cryptographic logic to encrypt and decrypt classified and sensitive unclassified information. The hardware or firmware is unclassified but controlled.

6-2. Because loss could compromise sensitive cryptographic technology, controlled cryptographic items are considered high-value, sensitive Army property that requires protection against unauthorized access. Unit COMSEC SOPs must address receiving, storing, and handling of controlled cryptographic items. The SOP contains instructions to secure devices to prevent loss or compromise

ACCOUNTABILITY

6-3. The CMCS has a central office of record and COMSEC accounting infrastructure at the depot, retail, and user levels. KOAMs manage the CMCS locally, and are accountable officers as defined in AR 735-5.

6-4. Property book officers account for controlled cryptographic items through the logistics system, not in COMSEC accounts. Property book officers list all controlled cryptographic items as class II and VII end items on property records and report controlled cryptographic item transactions in the Army central database. The property book officer records items by serial number and item unique identification and sends this information to the Army central database.

6-5. The United States Army Materiel Command Logistics Support Activity at Redstone Arsenal, Alabama manages the Army central database contract. Unless clearly defined in their contract, controlled cryptographic items for government contractors or vendors ship to the appropriate supporting Department of Defense activity address code or property book account.

SHIPMENT

6-6. All shipments of controlled cryptographic items transfer to an Army property book or Department of Defense activity address code account. Government contractors must obtain a Department of Defense activity address code to receive shipments of controlled cryptographic items.

6-7. Property book officers document the transfer of controlled cryptographic items from a contractor COMSEC account to an Army property book account using an SF 153. Upon receipt of a shipment of controlled cryptographic items, the receiving property book officer completes and signs the SF 153, and returns a copy to the originator. The Army property book officer maintains serial number accountability for all controlled cryptographic items.

6-8. The physical configuration and design of controlled cryptographic items determine their packaging and transportation requirements. During combat, in tactical situations, or during emergencies, shipping requirements may vary, based on risk assessments. COMSEC personnel should remove CIKs when transporting controlled cryptographic items. A qualified technician certified on DD Form 2625 (*Controlled Cryptographic Item Briefing*) inspects equipment before turn in or shipment and verifies the equipment is zeroized and the batteries removed.

STORAGE

6-9. Commanders should recognize that each additional high-value item in a secure storage facility increases the risk of loss by increasing the target potential. Units should not store controlled cryptographic items in vaults, security containers, or arms storage facilities containing items of monetary value, weapons, ammunition, high-pilferage items, or other sensitive items.

6-10. Controlled cryptographic items require security checks to ensure proper storage and safeguarding. Unkeyed controlled cryptographic items require safeguarding as sensitive but unclassified COMSEC equipment and require the same level of double-barrier protection provided desktop computers in offices; tactical radio sets installed in vehicles, shelters, or aircraft; and sensitive equipment in storage. Unattended security containers or vaults used to store classified COMSEC materials should remain locked, or use guards or an intrusion detection system. There is no security clearance requirement for access to unkeyed controlled cryptographic items. However, access is restricted to U.S. citizens with a valid need-to-know.

6-11. The handling or processing of keyed controlled cryptographic items does not take place through the logistics system. A controlled cryptographic item loaded with a key and with its associated CIK or card inserted assumes the security classification of the key and the material or information it protects. Personnel loading keying material into controlled cryptographic items must possess a security clearance equal to or higher than the classification of the key. There are no security clearance requirements to view COMSEC equipment where no opportunity exists for unauthorized access to the key or the input and output.

RELEASE AND ACCESS BY FOREIGN NATIONALS

6-12. The release of controlled cryptographic items is the responsibility of the Army Deputy Chief of Staff G-2 and the Army CIO/G-6. They share responsibilities and approval authority for the release of Army-owned COMSEC material to nonmilitary agencies, the general public, foreign nationals, or foreign governments. Release requests route through command channels to Headquarters, Department of the Army with justification.

6-13. Non-U.S. citizens, including foreign nationals and immigrant aliens employed by the United States, may receive limited access to unclassified controlled cryptographic items if the request for granting access is justified in writing based on operational needs. The command security authority decides to grant access based on a determination that the official duties of a foreign national requires this access. The controlled cryptographic items should not be in an environment that has an increased opportunity for foreign national access where the risk is unacceptable. If the material is classified, the commander requests limited access authorization in accordance with DODM 5200.02.

PROTECTIVE TECHNOLOGIES

6-14. The NSA provides tamper-revealing features for information processing equipment and keying material. The level of protection these products can provide depends on regular user inspection and controls. To ensure integrity of protective technologies, the KOAM oversees training in inspection and disposal of used protective technologies for personnel who routinely handle or use protectively packaged keying material or tamper-sealed information processing equipment.

***Note*.** The NSA provides technology pamphlets, tamper evident labels, tape, and bags free of charge. Ordering instructions are on the NSA Protective Technologies Website.

PERIODIC TAMPER CHECKS OF END CRYPTOGRAPHIC UNITS

6-15. All COMSEC devices require inspection for signs of tampering when delivered to a COMSEC account or property book account, upon maintenance turn in, upon recertification, and during a change of local element or KOAM inventory. Inspecting and dismounting connected devices may unintentionally zeroize the device or activate the tamper mode. To *zeroize* is to remove or eliminate the key from a cryptographic equipment or fill device (CNSSI 4009). Command inspections should include tamper checks of end cryptographic units. If inspection reveals evidence of tampering, the unit submits a COMSEC incident report. (Refer to AR 380-40.)

6-16. Evidence of device tampering or an attempt to open a device may include—

- Missing or loose screws.
- Bent, broken, or scratched metal access plates.
- Damaged tamper detection labels—
  - Missing, cut, or broken.
  - Discolored.
- Indicators and displays—
  - Indicators may flash or go out to indicate a tamper state.
  - The display screen may indicate a tamper state.

6-17. Indicators and displays may show false indications of a tamper state. Some devices default to tamper mode if they lose external power while their internal battery is inoperable. It is essential for account managers to know the tamper state of their equipment to maintain operational readiness. Operators should notify the commander, supervisor, and KOAM when there is an indication of tampering.

RECERTIFICATION AND REVALIDATION

6-18. COMSEC devices are subject to periodic recertification and validation. The KOAM determines which devices require certification. The KOAM should apply tamper detection labels according to NSA instructions. The certifying activities record the serial numbers of the labels applied to each device so the information is available to investigators if suspicion of tampering exists. Inspectors should compare recorded serial numbers with those removed from each device. Unexplained serial number discrepancies are reportable COMSEC incidents.

TRANSFER BETWEEN THE ARMY AND OTHER SERVICES

6-19. The Navy tracks controlled cryptographic items in the CMCS. Navy Department of Defense activity address codes are registered as user accounts, both locally and with the Navy central office of record.

6-20. The transfer of most controlled cryptographic items from the Air Force to the Army processes from the Air Force Equipment Management System to the Army property book officer, and should not involve the Air Force COMSEC account. All Services, agencies, and organizations other than the Army and Air Force use the CMCS to account for controlled cryptographic items.

6-21. Transfers of COMSEC equipment, including controlled cryptographic items, from Army elements to any other Service, agency, or organization, including the NSA, require Headquarters, Department of the Army approval and authorization in writing by the Wholesale National Inventory Control Point, Inventory Manager. AR 700-131 provides Army procedures for requesting approval for the loan of controlled cryptographic items.

6-22. Transfers to other Services and agencies use standard requisitioning and issuing procedures and documentation. The receiving agency assumes accountability for the controlled cryptographic items upon receipt into their COMSEC account. The receiving agency documents receipt using an SF 153. Refer to AR 700-131 for detailed procedures to transfer COMSEC equipment from Army inventory to other Services and agencies.

MAINTENANCE

6-23. Any individual authorized access to controlled cryptographic items may perform the operator preventive maintenance checks and services and operation test routines. Operators conduct maintenance according to instructions in the equipment technical manual.

6-24. Only trained maintainers with the appropriate security clearance who are certified on DD Form 1435 (*COMSEC Maintenance Training and Experience Record*) may remove protective covers and outer casings of controlled cryptographic items to perform field maintenance. The senior commander may authorize foreign nationals to perform limited maintenance on controlled cryptographic items only under direct supervision of the U.S. Government, U.S. Government contractor, or a vendor authorized to perform controlled cryptographic item maintenance.

6-25. Depot-level maintenance takes place at Tobyhanna Army Depot or a forward repair activity by technicians certified on DD Form 1435, except in forward areas of operations (refer to FM 4-0). AR 25-12 provides policy for the training and certification of communications-electronics maintenance technicians who perform COMSEC equipment maintenance. Forward repair activities provide on-site technical and logistical assistance to maintain and improve COMSEC and controlled cryptographic item performance.

6-26. Depot COMSEC reset returns equipment that has deployed to full operation. Accomplishing this may require equipment exchange, repair, or return. Reset prepares the unit for future operations by restoring equipment to full operation, normally within 180 days of redeployment. The typical turn-around time is 30–60 days after receipt of the equipment at the servicing depot-level maintenance facility.

Source Notes

This division lists sources by page number. Where material appears in a paragraph, it lists both the page number followed by the paragraph number.

Introduction: "A strong case can be made…": *A History of U.S. Communications Security (U): The David G. Boak Lectures, Vol. II*, National Security Agency, July 1981.

This page intentionally left blank.

Glossary

The glossary lists acronyms and terms with Army or joint definitions. Where Army and joint definitions differ, (Army) precedes the definition. ATP 6-02.75 is not the proponent for any Army terms. The proponent publication for terms is listed in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

ACES	Automated Communications Engineering Software
ADP	Army doctrine publication
ALC	accounting legend code
AR	Army regulation
ATP	Army techniques publication
CIK	cryptographic ignition key
CIO	chief information officer
CMCS	communications security material control system
CMDAUTH	command authority
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems instruction
COMSEC	communications security
CONAUTH	controlling authority
cryptonet	cryptographic net
CSLA	Communications Security Logistics Activity
DA	Department of the Army
DD	Department of Defense
DOC	document
DODI	Department of Defense instruction
DODM	Department of Defense manual
FIPS	federal information processing standards
FM	field manual
G-2	assistant chief of staff, intelligence
G-6	assistant chief of staff, signal
JP	joint publication
KEK	key encryption key
KMI	key management infrastructure
KOAM	key management infrastructure operating account manager
MGC	management client
NSA	National Security Agency
PAM	pamphlet

S-6	battalion or brigade signal staff officer
SF	standard form
SIPRNET	SECRET Internet Protocol Router Network
SKL	Simple Key Loader
SOI	signal operating instructions
SOP	standard operating procedure
TB	technical bulletin
TrKEK	transfer key encryption key
TSK	transmission security key
USB	universal serial bus

SECTION II – TERMS

accounting legend code

A numeric code used to indicate the minimum accounting controls required for items of accountable communications security material within the communications security material control system. Also called **ALC**. (CNSSI 4009)

administrative incident

A violation of procedures or practices dangerous to security that is not serious enough to jeopardize the integrity of a controlled cryptographic item, but requires corrective action to ensure the violation does not recur or possibly lead to a reportable COMSEC incident. (CNSSI 4001)

command authority

The command authority is responsible for the appointment of user representatives for a department, agency, or organization and their key and granting of modern (electronic) key ordering privileges for those user representatives. Also called **CMDAUTH**. (CNSSI 4005)

communications security

Actions designed to deny unauthorized persons information of value by safeguarding access to, or observation of, equipment, material, and documents with regard to the possession and study of telecommunications or to purposely mislead unauthorized persons in their interpretation of the results of such possession and study. Also called **COMSEC**. (JP 6-0)

communications security material control system

The logistics and accounting system through which communications security material marked CRYPTO is distributed, controlled, and safeguarded. Included are the communications security central offices of record, cryptologistic depots, and communications security accounts. Communications security material other than key may be handled through the communications security material control system. Electronic Key Management System and key management infrastructure are examples of tools used by the communications security material control system to accomplish its functions. Also called **CMCS**. (CNSSI 4005)

controlled cryptographic item

A secure telecommunications or information system, or associated cryptographic component, that is unclassified and handled through the communications security material control system, an equivalent material control system, or a combination of the two that provides accountability and visibility. (CNSSI 4009)

controlling authority

The official responsible for directing the operation of a cryptonet using traditional key and for managing the operational use and control of keying material assigned to the cryptonet. Also called **CONAUTH**. (CNSSI 4009)

cryptographic security

The component of communications security that results from the provision of technically sound cryptographic systems and their proper use. (CNSSI 4009)

emission security

Actions designed to deny unauthorized persons information of value as a result of intercept and analysis of compromising emanations from cryptographic equipment and telecommunications systems. (JP 6-0)

key management

The activities involving the handling of cryptographic keys and other related security parameters (e.g. passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and destruction. (CNSSI 4009)

key management infrastructure

The framework and services that provide the generation, production, storage, protection, distribution, control, tracking, and destruction for all cryptographic keying material, symmetric keys as well as public keys and public key certificates. Also called **KMI**. (CNSSI 4005)

key management infrastructure operating account manager

An external operational management role that is responsible for the operation of a key management infrastructure operating account that includes all distribution of key management infrastructure key and products from the management client to the end cryptographic units and fill devices, and management and accountability of all electronic and physical key, and physical communications materials from receipt and/or production to destruction or transfer to another key management infrastructure operating account. (Similar to an electronic key management system manager or communications security account manager.) Also called **KOAM**. (CNSSI 4005)

no-lone zone

An area, room, or space which, when manned, must be occupied by two or more appropriately cleared individuals who remain in sight of each other. (CNSSI 4009)

operational key

Key intended for over-the-air protection of operational information or the production or secure electrical transmission of key streams. (CNSSI 4009)

physical security

That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. (JP 3-0)

test key

Key intended for testing of communications security equipment or systems. If intended for off-the-air, in-shop use, such key is called maintenance key. (CNSSI 4005)

transmission security

Actions designed to protect transmissions from interception and exploitation by means other than cryptanalysis. (JP 6-0)

two-person integrity

The system of storage and handling designed to prohibit individual access to certain COMSEC keying material by requiring the presence of at least two authorized persons, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed. (CNSSI 4009)

user representative

The key management entity authorized by an organization and registered by the Central Facility Finksburg to order asymmetric key (including secure data network system key and message signature key). (CNSSI 4005)

zeroize

To remove or eliminate the key from a cryptographic equipment or fill device. (CNSSI 4009)

References

All URLs accessed 10 April 2020.

REQUIRED PUBLICATIONS

These documents must be available to intended users of this publication.

DOD Dictionary of Military and Associated Terms. January 2020.

ADP 1-02. *Terms and Military Symbols*. 14 August 2018.

FM 1-02.1. *Operational Terms*. 21 November 2019.

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

JOINT AND DEPARTMENT OF DEFENSE PUBLICATIONS

Most DOD publications are available at the DOD Issuances Website https://www.esd.whs.mil/DD/DoD-Issuances/.

DOD 5220.22M. *National Industrial Security Program Operating Manual*. 28 February 2006.

DODI 5200.33. *Defense Courier Operations (DCO)*. 30 June 2011.

DODI 8510.01. *Risk Management Framework (RMF) for DOD Information Technology (IT)*. 12 March 2014.

DODM 5200.02. *Procedures for the DOD Personnel Security Program (PSP)*. 3 April 2017.

Most joint publications are available at https://www.jcs.mil/doctrine.

JP 3-0. *Joint Operations*. 17 January 2017.

JP 6-0. *Joint Communications System*. 10 June 2015.

ARMY PUBLICATIONS

Army doctrinal and administrative publications are available at https://armypubs.army.mil.

ADP 1. *The Army*. 31 July 2019.

ADP 3-0. *Operations*. 31 July 2019.

ADP 3-90, *Offense and Defense*. 31 July 2019.

AR 25-2. *Army Cybersecurity*. 4 April 2019.

AR 25-12. *Communications Security Equipment Maintenance and Maintenance Training*. 23 December 2019.

AR 380-40. *Safeguarding and Controlling Communications Security Material (U)*. 9 July 2012.

AR 700-131. *Loan, Lease, and Donation of Army Materiel*. 23 August 2004.

AR 710-2. *Supply Policy Below the National Level*. 28 March 2008.

AR 735-5. *Property Accountability Policies*. 9 November 2016.

ATP 4-33. *Maintenance Operations*. 9 July 2019.

DA PAM 25-2-16. *Communications Security (COMSEC)*. 8 April 2019.

FM 3-0. *Operations*. 6 October 2017.

FM 6-02. *Signal Support to Operations*. 13 September 2019.

FM 6-27. *The Commander's Handbook on the Law of Land Warfare*. 7 August 2019.

TB 380-41. *Security: Procedures for Safeguarding, Accounting, and Supply Control of COMSEC Material*. 15 August 2013.

OTHER PUBLICATIONS

A History of U.S. Communications Security (U): The David G. Boak Lectures, Vol. II. National Security Agency, July 1981. https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-histories/history_comsec_ii.pdf.

Committee on National Security Systems publications can be found online at: https://www.cnss.gov/CNSS/issuances/instructions.cfm.

CNSSI 4001. *Controlled Cryptographic Items.* 7 May 2013.

CNSSI 4005. *Safeguarding Communications Security (COMSEC) Facilities and Materials*. 22 August 2011.

CNSSI 4009. *Committee on National Security Systems (CNSS) Glossary*. 6 April 2015.

Committee on National Security Systems Policy No. 3. *National Policy on Granting Access to U.S. Classified Cryptographic Information*. 01 October 2007. https://www.cnss.gov/CNSS/issuances/Policies.cfm.

FIPS PUB 140-3. *Security Requirements for Cryptographic Modules*. 22 March 2019. https://csrc.nist.gov/publications/fips.

NAG-16F. *(U) Field Generation and Over-the-Air Distribution of COMSEC Key in Support of Tactical Operations and Exercises*. May 2001. https://csla.army.mil/Sections/COMSEC/DocNSA.aspx.

RECOMMENDED READINGS

ATP 3-39.32. *Physical Security.* 30 April 2014.

FM 3-12. *Cyberspace and Electronic Warfare Operations*. 11 April 2017.

TB 380-40. *Security: Army Controlling Authority and Command Authority Procedures*. 10 September 2012.

NSA/CSS Policy Manual 9-12. *NSA/CSS Storage Device Sanitization Manual*. 15 December 2014. https://www.nsa.gov/Resources/Everyone/Media-Destruction/.

PRESCRIBED FORMS

This section has no entries.

REFERENCED FORMS

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website at https://armypubs.army.mil. DD forms are available on the Executive Services Directorate website at https://www.esd.whs.mil/Directives/forms. SFs are available on the U.S. General Services Administration website at https://www.gsa.gov/reference/forms.

DA Form 2028. *Recommended Changes to Publications and Blank Forms*.

DA Form 5941-R. *COMSEC Material Disposition Record.*

DD Form 254. *Department of Defense Contract Security Classification Specification*.

DD Form 1435. *COMSEC Maintenance Training and Experience Record*.

DD Form 2625. *Controlled Cryptographic Item (CCI) Briefing*.

SF 153. *COMSEC Material Report.*

WEBSITES

Army Cryptographic Modernization Website. http://csla.army.mil/Sections/Cryptomod/cryptomod.aspx (requires DOD-approved certificate login).

Army Cybersecurity One Stop Shop Portal. https://www.milsuite.mil/wiki/Portal:Army_Cybersecurity (requires DOD-approved certificate login).

Army Key Management Website. https://csla.army.mil/Sections/KMT/KMI.aspx (requires DOD-approved certificate login).

Communications Security Logistics Activity Website. https://csla.army.mil/ (requires DOD-approved certificate login).

NSA Protective Technologies Website https://apps.nsa.gov/iaarchive/products-services/products/protective-technologies.cfm.

This page intentionally left blank.

Index

Entries are by paragraph number.

ATP 6-02.75
18 May 2020

By Order of the Secretary of the Army:

JAMES C. MCCONVILLE
General, United States Army
Chief of Staff

Official:

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army
2013610

DISTRIBUTION:
Distributed in electronic media only(EMO).

This page intentionally left blank.

PIN: 105459-000