SUBCOURSE
SS0137

EDITION
A

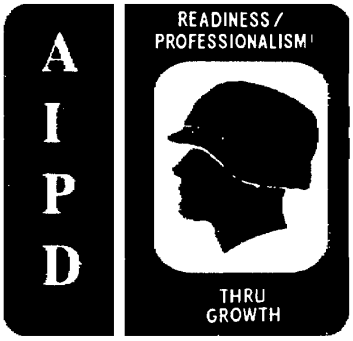
US ARMY SIGNAL CENTER AND FORT GORDON

COMMUNICATIONS SECURITY
(SC 25C-RC)

EDITION DATE: SEPTEMBER 1994

THE ARMY INSTITUTE FOR PROFESSIONAL DEVELOPMENT

ARMY CORRESPONDENCE COURSE PROGRAM



COMMUNICATIONS SECURITY

Subcourse SS 0137

Edition A

United States Army Signal Center and Fort Gordon
Fort Gordon, Georgia 30905-5000

7 Credit Hours

Edition Date: September 1994

SUBCOURSE OVERVIEW

This subcourse is designed to teach about communications security (COMSEC), including COMSEC custodian duties, identifying COMSEC material, cryptofacility approval, physical security of COMSEC material and keys, COMSEC accountability, COMSEC emergency plans, and COMSEC-related inspections and audits.

The prerequisite for this subcourse is that you are a graduate of the Signal Officer Basic Course or its equivalent.

This subcourse reflects the doctrine which was current at the time it was prepared. In your own work situation, always refer to the latest official publications.

Unless this publication states otherwise, masculine nouns and pronouns do not refer exclusively to men.

TERMINAL LEARNING OBJECTIVE

ACTION: Describe the duties involved in managing a COMSEC account.

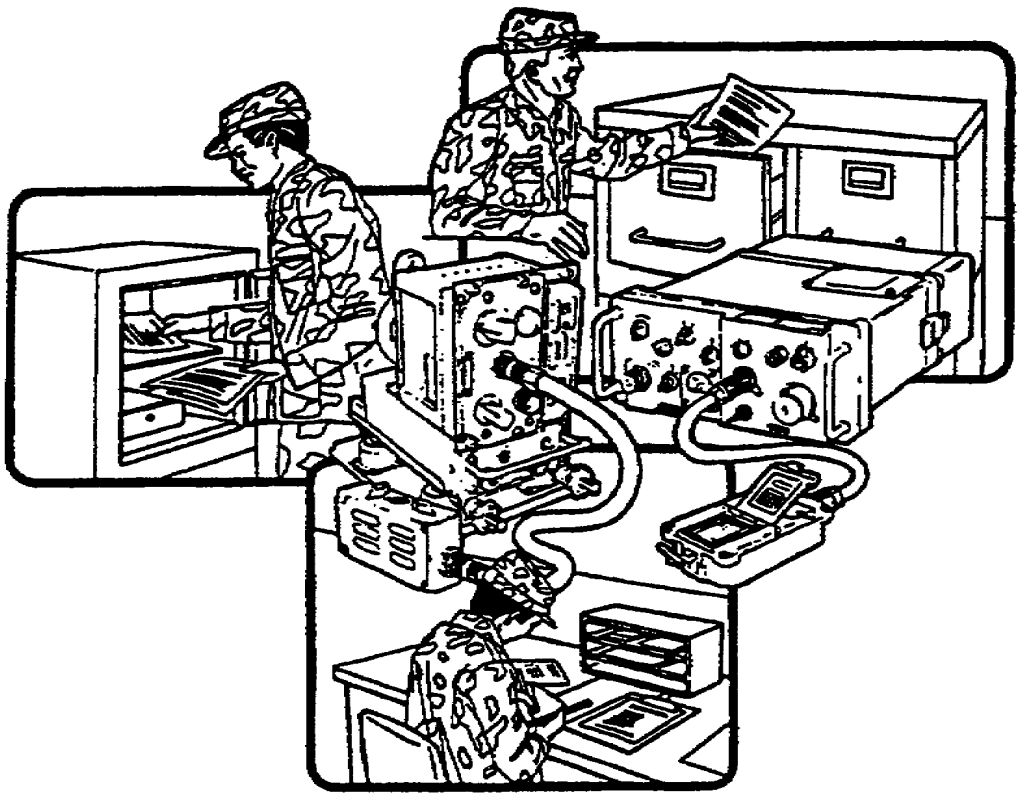
CONDITION: Given this subcourse.

STANDARD: To demonstrate competence on this task, you must achieve a minimum of 70 percent on the subcourse examination.

TABLE OF CONTENTS

LESSON 1

PURPOSE OF
COMMUNICATIONS SECURITY



FOR OFFICIAL USE ONLY

LESSON 1

PURPOSE OF COMMUNICATIONS SECURITY

CRITICAL TASKS: 01-5770.07-9001
01-5879.07-9001

OVERVIEW

LESSON DESCRIPTION:

In this lesson, you will learn about COMSEC, to include its purpose and the threat it counters.

TERMINAL LEARNING OBJECTIVE:

ACTION: Describe the purpose of COMSEC, its vulnerabilities, and countermeasures.

CONDITION: Given this lesson.

STANDARD: To demonstrate competence, you must achieve a minimum of 70 percent on the subcourse examination.

REFERENCES: The material in this lesson was derived from the following publications: AR 380-5, AR 380-19, FM 24-1, FM 100-5, and TB 380-41 series.

INTRODUCTION

A battle's outcome often depends on the security, quality, and timeliness of communications. Only the enemy is totally aware of the quality of our COMSEC. Every soldier must be trained to understand the importance of maintaining secure communications. Soldiers' lives depend on effective COMSEC. The weaker our COMSEC efforts, the easier it is for an enemy to exploit our communications.

1. General. All electrical devices produce some form of emissions. Certain devices can capture those emissions, sort them, determine their general origin, and determine their meanings. These emissions have two forms. Some involve communications (radio) and others do not (radar and so forth). The gathering and interpreting of these missions are called communications intelligence and electronic intelligence. However, complex systems and techniques to intercept and interpret these emissions are not needed if basic COMSEC practices are ignored.

2. Communications security. COMSEC is the protection resulting from measures designed to deny unauthorized persons information of value gained from having access to and studying our communications. It involves ensuring the authenticity of such communications. Figure 1-1 shows the COMSEC elements.

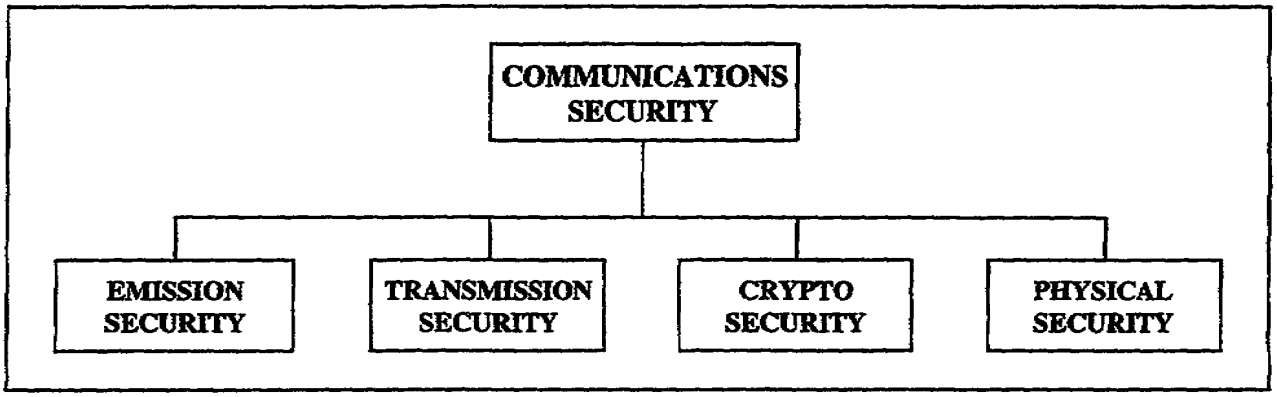


Figure 1-1. COMSEC elements.

a. Emission security helps deny information from unauthorized persons. An enemy will likely intercept what is sent. One method is to observe total silence. This involves turning off all radiating systems. Another is selective silence where only certain systems operate during specific periods. An enemy unit that does not know about a friendly unit cannot get targeting or other data. Denial is easier when operators:

(1) Mask antenna locations.

(2) Use directional antennas.

(3) Keep transmissions as short as possible.

(4) Use the minimum power needed to pass information.

b. Transmission security (TRANSEC) protects transmissions from being intercepted and exploited, except by cryptoanalysis.

(1) The key to TRANSEC is organized, succinct, and well thought out messages to keep transmission time to a minimum. Give only what is needed to those who need it

Try to keep transmissions to 15 seconds or less. Longer periods increase the odds an enemy will intercept and exploit a message.

(2) Poor TRANSEC may make the sending unit an information source for an enemy. The enemy may not target that unit for destruction until it outlives its usefulness.

(3) Operators must avoid unauthorized discussions and chatter. Trained enemy signal analysts can exploit them. Topics for operators to avoid include:

(a) Locations and equipment.

(b) Communication problems.

(c) Morale and operations.

c. Cryptosecurity uses approved systems to keep communications secure. Cryptosecurity involves:

(1) Providing technically sound cryptosystems.

(2) Ensuring their proper use.

d. Physical security involves protecting equipment, material, and documents from access or observation by unauthorized persons. Some possible threats are loss, theft, sabotage, and unauthorized access.

3. COMSEC material.

a. COMSEC material is used to protect communications and ensure their authenticity. It has two categories.

(1) COMSEC equipment refers to all COMSEC hardware. This includes equipment end items, components, and repair parts.

(2) COMSEC key and publications include COMSEC material, except equipment, that performs or helps perform cryptographic functions. Examples are forms of COMSEC keying material, call frequency systems, and COMSEC publications.

b. The following help to identify COMSEC material:

(1) The Army Master Data File (AMDF) lists catalog data for all equipment.

(2) The COMSEC Material Management Data Catalog lists catalog data for all COMSEC material. It is referred to as the ARKAG 2.

(3) Critical data elements help to identify COMSEC items.

(a) The accounting legend code (ALC) identifies how an item must be accounted for in the COMSEC Material Control System (CMCS). The ARKAG 2 lists the ALC.

(b) The controlled item inventory code (CIIC) identifies an item's classification. The AMDF lists the CIIC for COMSEC equipment.

(c) The security classification code (SCC) also identifies an items classification. The ARKAG 2 lists the SCC for COMSEC material.

(d) The AMDF lists the source of supply.

4. Controlling activities. The CMCS is the logistic system for distributing, controlling, and safeguarding accountable COMSEC material. It consists of the Army COMSEC Central Office of Record (ACCOR), depot, accounts, and subaccounts.

a. The ACCOR maintains records of centrally accountable COMSEC material. It also monitors accounting procedures and audits COMSEC accounts within the Army.

b. The Army COMSEC Commodity Logistic Accounting and Information Management System (ACCLAIMS) is an automated system. It reports COMSEC transactions within the CMCS. The ACCLAIMS is divided into four levels by location.

(1) Level 1-Communications-Electronics Command COMSEC Logistics Activity (CCSLA). The CCSLA has the worldwide mission of COMSEC logistic support. To do this, there are COMSEC logistic support facilities. They include support centers and support units.

(2) Level 2-Blue Grass Army Depot

(3) Level 3--Theater COMSEC Logistics Support Center, Europe.

(4) Level 4-User COMSEC accounts.

c. The controlling authority is the commander of the organization or activity responsible for setting up and operating a cryptonet.

5. Responsibilities.

a. Final responsibility for safeguarding COMSEC material rests with the commander.

(1) A commander ensures COMSEC accounts and facilities receive command COMSEC inspections. These should be done at least once every 24 months.

(2) A commander appoints a COMSEC custodian and at least one alternate for each COMSEC account in his command. The COMSEC custodian and alternates are

officers or warrant officers (if possible). Appointed enlisted personnel must be at least a staff sergeant for custodian and sergeant for alternate.

b. Individual users must physically protect COMSEC material in their possession or under their control. They have the primary responsibility for reporting any occurrence, circumstance, or act that could jeopardize the security of COMSEC material. They also follow the COMSEC custodian's instructions for protecting and controlling material.

6. COMSEC custodian duties. A COMSEC custodian is responsible for actions concerning accountable COMSEC material charged to his account. The custodian routinely does:

a. Material receipt. He formally acknowledges receiving keying material, publications, and equipment.

b. Inventory. He makes sure that COMSEC inventories of material and equipment are conducted. He also makes sure daily or shift-to-shift and other periodic inventories are conducted.

c. Transfer. He ensures that transfers of accountable material are properly reported and recorded.

d. Accounting. He makes sure material is accounted for, from receipt through final disposition. He keeps publications current and promptly posts amendments.

e. Destruction. He makes sure COMSEC facility personnel are thoroughly familiar with emergency destruction procedures.

f. Reports. He submits timely routine reports on the status of COMSEC material.

7. COMSEC keying process.

a. COMSEC key is a sequence of random binary bits used to set up initially, and change periodically, permutations in crypto equipment. They are used to encrypt and decrypt electronic signals, control TRANSEC processes, and produce other keys.

b. Cryptosystems provide security by preventing unauthorized persons from receiving information sent electronically. Authentication systems help defend against enemy intrusion into communications nets. These systems help to establish the authenticity of stations, communications, or operators. Both systems are needed to have adequate operations security. Homemade authentication code systems are never allowed. The only Army-approved systems are:

(1) Those produced by the National Security Agency (NSA). They are obtained through Army channels.

(2) Those that the Intelligence and Security Command (INSCOM) produces to meet an emergency need.

c. Authority to receive COMSEC keying material or publications is based on a unit's operational and support needs. Regularly superseded keying material is automatically resupplied based on the supersession rate and distribution schedule. Procedures for obtaining this material are in TB 380-41, Procedures for Safeguarding, Accounting and Supply Control of COMSEC Material.

8. Summary.

a. Electronic devices produce emissions. These may or may not involve communications.

b. COMSEC equipment refers to all COMSEC hardware. COMSEC key and publications include all COMSEC material except equipment. Critical data elements help to identify COMSEC items.

c. Accountable COMSEC material is distributed, controlled, and safeguarded through the CMCS.

d. Safeguarding COMSEC material is a command responsibility.

e. COMSEC custodians and alternates are officers or warrant officers, if possible.

THIS PAGE INTENTIONALLY LEFT BLANK

LESSON 1

PRACTICE EXERCISE

The following items will test your grasp of the material covered in this lesson. There is only one correct answer for each item. When you complete the exercise, check your answers with the answer key that follows. If you answer any item incorrectly, study again that part of the lesson which contains the portion involved.

1. What is the key to effective TRANSEC?

   A. Keeping transmission time to a minimum

   B. Siting antenna properly

   C. Using minimum power to transmit

   D. Using proper authentication procedures

2. Who has final responsibility for safeguarding COMSEC material?

   A. Signal officer

   B. COMSEC custodian

   C. Alternate COMSEC custodian

   D. Commander

3. Who has the primary responsibility for reporting an act that could jeopardize the security of COMSEC material?

   A. COMSEC custodian

   B. Commander

   C. COMSEC alternate custodian

   D. Individual user

4. What is a sequence of random binary bits that are used to encrypt and decrypt electronic signals?

   A. COMSEC custodian

   B. COMSEC key

   C. COMSEC publications

   D. COMSEC material

5. When can a homemade code system be used?

   A. Only in emergency situations

   B. At brigade level and below

   C. At division level and higher

   D. Never

LESSON 1

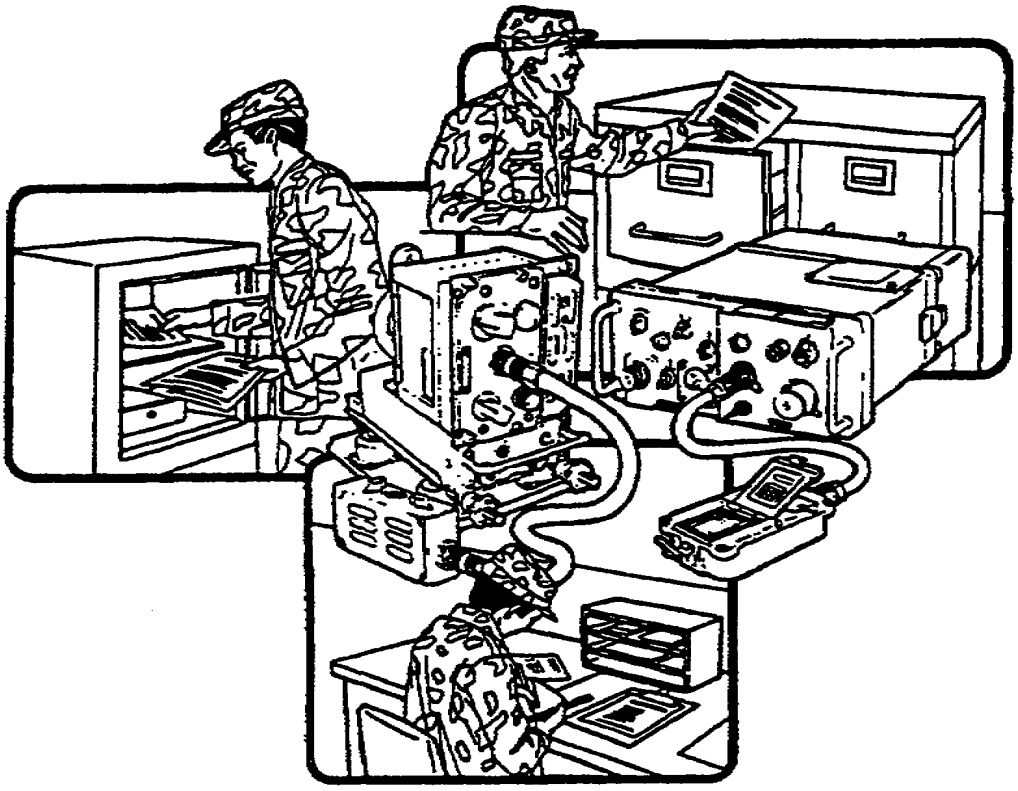
PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

Item	Correct Answer and Feedback
1.	A. Keeping transmission time to a minimum The key to TRANSEC is organized, succinct, and well thought out messages to keep transmission time to a minimum (page 1-2, para 2b(1)).
2.	D. Commander Final responsibility for safeguarding COMSEC material rests with the commander (page 1-4, para 5a).
3.	D. Individual user Individual users have the primary responsibility for reporting any occurrence, circumstance, or act that could jeopardize the security of COMSEC material (page 1-5, para 5b).
4.	B. COMSEC key COMSEC key is a sequence of random binary bits used to set up initially, and change periodically, permutations in crypto equipment (page 1-5, para 7a).
5.	D. Never Homemade authentication code systems are never allowed (page 1-5, para 7b).

LESSON 2

ESTABLISHING A CRYPTOFACILITY



FOR OFFICIAL USE ONLY

LESSON 2

ESTABLISHING A CRYPTOFACILITY

CRITICAL TASKS: 01-5770.07-9001
01-5879.07-9001

OVERVIEW

LESSON DESCRIPTION:

In this lesson, you will learn about establishing a cryptofacility.

TERMINAL LEARNING OBJECTIVE:

ACTION: Describe how to establish a cryptofacility.

CONDITION: Given this lesson.

STANDARD: To demonstrate competence, you must achieve a minimum of 70 percent on the subcourse examination.

REFERENCES: The material in this lesson was derived from the following publications: AR 190-13, AR 190-16, and TB 380-41 series.

INTRODUCTION

A cryptofacility provides the physical security needed to protect COMSEC material from loss or compromise. It can be fixed, transportable, or mobile. The U.S. Army INSCOM must approve a fixed facility used for holding or using classified COMSEC material. Commanders are responsible for verifying the proper handling and protection of COMSEC material held in mobile and transportable facilities. This applies to facilities that are operational for less than 90 days.

1. Cryptofacility. A cryptofacility is any facility that is used for operating, maintaining, and storing COMSEC material.

a. Fixed facilities include vaults in buildings or other immovable structures. There are six types of fixed facilities.

(1) An attended facility is manned by full or part-time operators.

(2) An unattended facility is not manned. It has some storage restrictions. For example, future keying material cannot be stored in it.

(3) A contingency facility contains a full or a partial set of crypto equipment. The equipment is in an operational configuration awaiting rapid activation. Keying material cannot be stored in this facility.

(4) A secure subscriber terminal is a secure facility located within another structure in which user-operated secure voice, data, facsimile, or video circuits terminate. This facility is usually found in a permanent headquarters. It is seldom found in a maneuver battalion or brigade area.

(5) A special multichannel terminal uses crypto equipment to protect multichannel trunks that pass classified or unclassified information.

(6) A storage facility exists solely for string COMSEC equipment. It can be a security container approved by the General Services Administration (GSA). If so, it must be in an area that has secondary barriers against unauthorized access.

b. Transportable and mobile facilities are operational for periods of 90 days or less. They hold COMSEC material on hand receipt. The commander is responsible for security management of these facilities.

2. Identification. External identification is limited to avoid advertising what is in a particular facility. Only a RESTRICTED AREA sign and a warning notice are posted on a facility's door. The signs are bilingual where appropriate.

3. Approval requests.

a. INSCOM approve any fixed COMSEC facility used for operating, maintaining, distributing, storing, or research-development sting and evaluation of accountable COMSEC material. Approval must be received before:

(1) Establishing a fixed facility.

(2) Making major alterations that affect a fixed facility's physical security.

(3) Relocating a fixed facility.

(4) Upgrading a fixed facility's classification.

b. The local commander submits the request for a fixed facility through normal command channels to the appropriate INSCOM signal security support unit. The request contains the following information (if applicable).

(1) Requesting unit’s complete address.

(2) Unit identification code (UIC).

(3) Telephone (DSN and commercial).

(4) COMSEC account number (if the unit has one).

(5) Facility location. For example, the building floor, and room number.

(6) Point of contact and telephone number.

(7) Type of request (initial request, update, and so forth).

(8) Classification information. This is the highest classification for the COMSEC material that will be used or stored.

c. The approving authority needs to know about the facility's physical characteristics.

(1) State whether the facility is fixed, mobile, or transportable. If it is not fixed, identify its configuration by nomenclature.

(2) State the facility's primary purpose. This is based on:

(a) Operations (supporting crypto operations).

(b) Distribution. For example, its primary mission will be COMSEC logistic support. That is, it will be a COMSEC logistic support facility (CLSF).

(c) Maintenance. For example, a direct support activity.

(d) Research-development-testing and evaluation.

(e) Administrative. This is set up for holders of accountable COMSEC material. It is used for reference.

(f) Storage. This involves short or long-term storage between operational use in a tactical environment, for training, or for exercises.

(g) Other (explain).

(3) Identify the general cryptosystems held or requested. The mythological designator (NESTOR or VINSON) identifies these. If no designator is available, identify the equipment by its short title and end item.

(4) Describe the planned physical security measures. These include the overall construction, walls, ceilings, floors, windows, door, access control, and other measures to

prevent overt or covert access. Provide the GSA description of the vault door lock (if applicable). Also describe the security containers used in the facility.

(5) Describe how classified COMSEC items will be protected during nonworking hours. Also describe their protection when not under the direct and continuous control of proper cleared and authorized persons. Protection methods include approved containers, vaults, strong rooms, and so forth.

(6) State whether applicable standards for operating, storing, and destroying COMSEC material can be met.

4. Approving authority action.

a. INSCOM notifies the requesting commander and the ACCOR whether the facility request is approved. This is based on information in the approval request and an INSCOM inspection.

b. If not approved, INSCOM states the actions needed to get approval. The CLSF will not issue COMSEC material to a unit until its COMSEC account is set up.

5. Cryptofacility reapproval.

a. A facility's approval is valid as long as its physical security features remain basically unchanged.

b. When those physical security features change, and the facility is still needed, a reapproval process begins. The organization sends its request through channels to the approving authority, which is INSCOM.

c. A facility's approval may be invalidated. When this occurs, the approving authority notifies the ACCOR and other agencies. This ensures COMSEC material is not sent to the facility in question until approval is restored.

d. The approving authority may consider a facility's protection to be inadequate. If so, all COMSEC material in the facility must be returned to the proper authority or securely stored.

6. Summary.

a. A cryptofacility is any facility that is used for operating, maintaining and storing COMSEC material. It can be fixed, mobile, or transportable.

b. External identification is limited to avoid advertising what is in a particular facility.

c. The commander submits the facility request.

d. INSCOM approval must be received before:

(1) Establishing a fixed facility.

(2) Making major alterations that affect a fixed facility's physical security.

(3) Relocating a fixed facility.

(4) Upgrading the classification of a fixed facility.

e. A facility's approval is valid as long as its physical security features remain basically unchanged.

LESSON 2

PRACTICE EXERCISE

The following items will test your grasp of the material covered in this lesson. There is only one correct answer for each item. When you complete the exercise, check your answers with the answer key that follows. If you answer any item incorrectly, study again that part of the lesson which contains the portion involved.

1. Which agency approves the request to upgrade a cryptofacility?

   A. Forces Command

   B. Information Systems Command

   C. Intelligence and Security Command

   D. Training and Doctrine Command

2. What are the three general cryptofacility configurations?

   A. Attended, unattended, and contingency

   B. Brigade, divisional, and corps

   C. Fixed, mobile, and transportable

   D. Tactical, operational, and strategic

3. A COMSEC storage facility exists solely for storing COMSEC equipment. Which statement describes such a facility?

   A. It may consist of a GSA-approved security container if the container is in an area that provides secondary barrier against unauthorized access

   B. It may consist only of a GSA-approved security container

   C. It does not have the same degree of physical protection as a fixed cryptofacility

   D. It must receive the same degree of physical protection as a mobile cyptofacility

4. How should a cryptofacility be marked to keep unauthorized persons from entering it?

   A. NO ADMITTANCE WITHOUT PROPER CLEARANCE VERIFICATION sign

   B. COMSEC FACILITY-DO NOT ENTER sign

   C. COMSEC AREA sign, with an appropriate warning notice

   D. RESTRICTED AREA sign, with an appropriate warning notice

5. When is the approval of a fixed cryptofacility obtained?

   A. During the planning stages

   B. After it is built and the COMSEC account is in place

   C. Before establishing a facility, before major alterations that affect physical security, or when relocating a facility

   D. Before it is built, provided the construction plans meet INSCOM specifications

6. On what is INSCOM approval of a cryptofacility based?

   A. Recommendation of the local commanding officer

   B. Current worldwide threat analysis

   C. An evaluation of the information in the facility approval request and an inspection by the approving authority

   D. The record of COMSEC violations within the command over the previous three fiscal years

7. How often must a cryptofacility obtain reapproval?

   A. Every 6 months

   B. Every year

   C. Every 2 years

   D. It is not needed as long as its physical features are unchanged

LESSON 2

PRACTICE EXERCISE

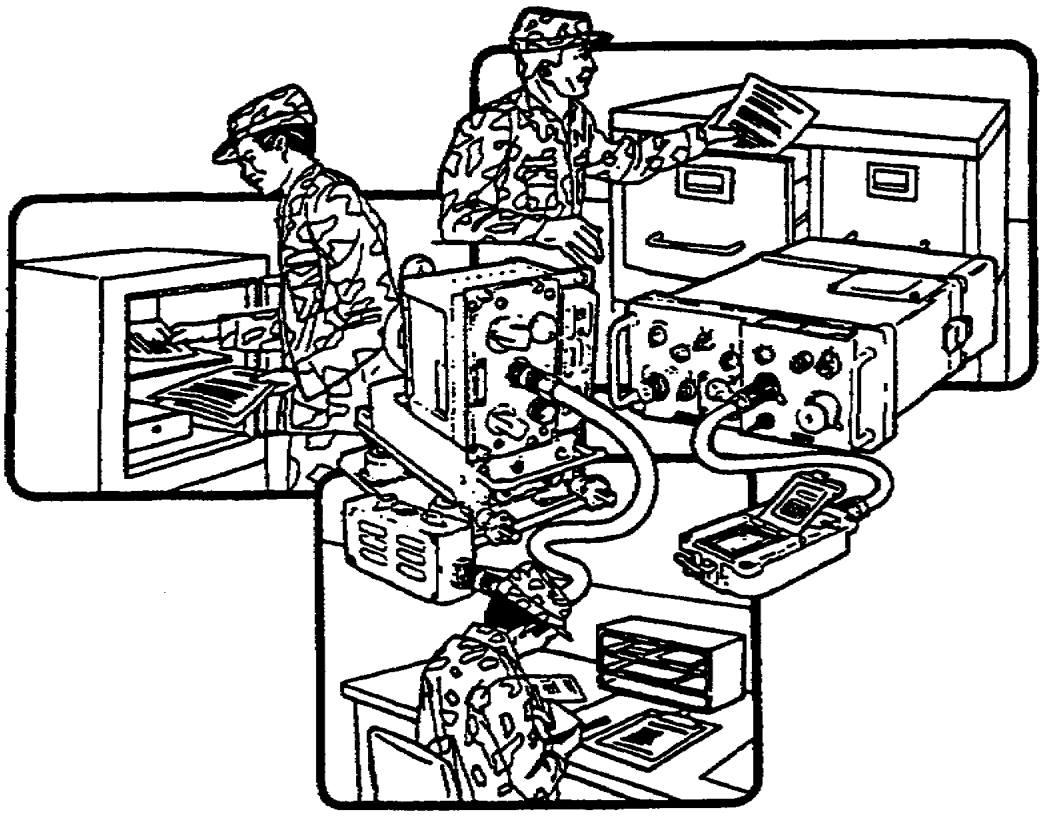
ANSWER KEY AND FEEDBACK

Item	Correct Answer and Feedback
1.	C. Intelligence and Security Command The U.S. Army INSCOM approves any fixed COMSEC facility used for operating, maintaining, distributing, storing, or research-development-testing and evaluation of accountable COMSEC material (page 2-2, para 3a(4)).
2.	C. Fixed, mobile, and transportable The three general cryptofacility configurations are fixed, mobile, and transportable (page 2-1, para 1a and 1b).
3.	A. It may consist of a GSA-approved security container if the container is in an area that provides secondary barriers against unauthorized access A COMSEC storage facility may consist of a GSA-approved security container if the container is in an area that provides secondary barriers against unauthorized access (page 2-2, para 1a(6)).
4.	D. RESTRICTED AREA sign, with an appropriate warning notice A cryptofacility should have a RESTRICTED AREA sign, with a warning notice, to keep unauthorized persons from entering it (page 2-2, para 2).
5.	C. Before establishing a facility, before major alterations that affect physical security, or when relocating a facility The approval of a fixed cryptofacility is obtained before establishing a facility, before major alterations that affect physical security, or when relocating a facility (page 2-2, para 3a, 3a(1), 3a(2), and 3a(3)).
6.	C. An evaluation of the information in the facility approval request and an inspection by the approving authority INSCOM approval of a cryptofacility is based on an evaluation of the information in the facility approval request and an inspection by the approving authority (page 2-4, para 4a).

Item	Correct Answer and Feedback
7.	D. It is not needed as long as its physical features are unchanged A facility's approval is valid as long as its physical security features remain basically unchanged (page 2-4, para 5a).

LESSON 3

IDENTIFYING COMMUNICATIONS SECURITY MATERIAL



FOR OFFICIAL USE ONLY

LESSON 3

IDENTIFYING COMMUNICATIONS SECURITY MATERIAL

CRITICAL TASKS: 01-5770.07-9001
01-5879.07-9001

OVERVIEW

LESSON DESCRIPTION:

In this lesson, you will learn the special markings and designators that identify COMSEC materials.

TERMINAL LEARNING OBJECTIVE:

ACTION: Identify COMSEC special markings, designators, acronyms, and references.

CONDITION: Given this lesson.

STANDARD: To demonstrate competence, you must achieve a minimum of 70 percent on the subcourse examination.

REFERENCES: The material in this lesson was derived from the following publications: AR 380-5, AR 380-19, AR 380-40, and TB 380-41 series.

INTRODUCTION

COMSEC material and equipment must be protected properly. This is due to its sensitive and vital role in secure communications. The security of COMSEC material is based on preventing unauthorized access. Special markings and designators help provide the degree of security needed.

1. General. COMSEC material is used to protect communications and ensure their authenticity. It has two groups.

a. One group is COMSEC key and publications. These include COMSEC material, other than equipment, that does or helps to do cryptographic functions. These include keying items, call sign systems, and COMSEC publications.

b. The second group is COMSEC equipment. This refers to COMSEC hardware. It includes equipment end items, components, and repairs parts. The NSA determines the classification of all COMSEC equipment.

2. COMSEC terms. To identify COMSEC material, you must know its related terms.

a. Key refers to a sequence of randomly-generated binary bits. They are used to encrypt and decrypt electronic signals. A keys classification equals the highest classification of the data being encrypted. Classified keys are not downgraded or declassified without written approval from the controlling authority. The four major key types are:

(1) Traffic encryption key. This encrypts and decrypts plain text and encrypted data.

(2) Key encryption key. This encrypts and decrypts other keys for transmission or storage.

(3) Transmission security key. This controls transmission security processes.

(4) Key production key. This is used to initialize a key generator for producing other electronically generated keys.

b. CRYPTO identifies COMSEC keying that protects or authenticates communications. Written items are marked CRYPTO only if they contain crypto key information. The term CRYPTO is always capitalized. It identifies keying material handled under the special access, storage, distribution, accounting, and destruction requirements of the CMCS. Most hard copy key produced by the NSA is marked CRYPTO. It is used on both classified and unclassified key. It is not used on equipment, manuals, or other COMSEC material.

c. Controlled cryptographic items (CCI) are secure telecommunications or information handling equipment. They also include associated crypto components and common fill devices. CCI are unclassified when unkeyed, but they are still controlled. Equipment, components, and fill devices so designated bear the designator controlled cryptographic item or CCI.

d. A COMSEC incident is an occurrence that could jeopardize COMSEC material or secure COMSEC. Examples are lost COMSEC material and unauthorized persons who gain access to classified COMSEC material.

e. A COMSEC insecurity is any investigated or evaluated incident which has been determined to jeopardize the security integrity of COMSEC material or the secure transmission of government data.

(1) A physical incident is the loss, theft, loss of control, capture, recovery by salvage, tampering, or unauthorized viewing, access, or photography of classified

COMSEC material or unclassified COMSEC key marked CRYPTO. It is also the loss, theft, capture, recovery by salvage, or tampering of unclassified keyed CCI.

(2) A personnel incident occurs when a person with access to classified COMSEC information is suspected of espionage, defection, subversion, or sabotage. It also includes deliberate or accidental disclosure of that information to an unauthorized person. Other examples are the capture, unauthorized absence, or the revocation of a clearance for cause of a person having detailed knowledge of COMSEC matters.

(3) A cryptographic incident is any equipment malfunction or crypto-operator error. These may help unauthorized persons recover the message texts, or the key to a cryptosystem through cryptoanalytic methods.

3. COMSEC material control system. COMSEC material has its own logistics system.

a. Accountable material is distributed, controlled, and protected using the CMCS. It includes ACCOR, depots, and COMSEC accounts and subaccounts.

b. Reportable material is accountable COMSEC material that needs periodic inventory and reconciliation with ACCOR. This ensures strict accounting and centralized control. Keying material is also controlled in the CMCS.

4. COMSEC material management data catalog. Known as ARKAG 2, it lists catalog data for all COMSEC material. The critical data elements are noted for each item in ARKAG 2.

a. The ALC identifies accountability requirements in the CMCS.

b. The CHIC identifies the classification of an item. The AMDF lists the CC for COMSEC equipment. The AMDF also lists the source of supply for COMSEC equipment.

c. The SSC also identifies the classification of an item.

5. COMSEC classifications. COMSEC custodians must know how to protect and control COMSEC material. Proper handling ensures proper safeguarding.

a. COMSEC information cannot be released to foreign nationals unless authorized by the Deputy Chief of Staff for Intelligence, Headquarters, Department of the Army (HQDA). This applies even if NOFORN (not releasable to foreign nationals) is not on a document.

b. FOR OFFICIAL USE ONLY (FOUO) is a protective marking. It applies to unclassified material meant only for official use. Thus, it should have no public disclosure. That includes open and public displays at nongovernmental meetings or open houses. Requests for public release of FOUO items are referred to HQDA. These include Freedom of Information Act requests. FOUO is usually used for unclassified COMSEC information. FOUO should be used for several purposes.

(1) A list of COMSEC short or long titles.

(2) Narrative technical data on the characteristics of crypto equipment.

(3) Indications of new COMSEC developments.

(4) COMSEC planning and budgeting information.

(5) Handling instructions and doctrinal information related to COMSEC material.

(6) Manual cryptosystems produced exclusively for unclassified training purposes.

(7) Unclassified COMSEC material reports.

c. COMSEC material may be classified CONFIDENTIAL, SECRET, or TOP SECRET. Personnel must have a security clearance equal to or higher than the material they are using.

d. Unless stated otherwise COMSEC equipment and information are classified indefinitely. For COMSEC-related documents prepared from multiple sources, the declassification date or event with the longest classification period applies.

6. References. The following references govern COMSEC procedures. They apply to military and civilian members of the active and reserve components.

a. AR 380-5, Department of the Army Information Security Program. This sets the policies and procedures for classifying, downgrading, and declassifying sensitive information.

b. AR 380-19, Information Systems Security. This covers COMSEC, computer security (COMPUSEC), and electronic security (ELSEC). It also introduces information systems security (ISS) as a discipline. ISS includes COMSEC, COMPUSEC, ELSEC, and the control of compromising emanations (TEMPEST). It provides minimum security standards for sending classified and sensitive unclassified data.

c. AR 380-40, Policy for Safeguarding and Controlling COMSEC Material. This states Army policy for protecting and controlling COMSEC material. It applies to non-Army elements that have Army COMSEC accounts.

d. TB 380-41 series, Procedures for Safeguarding, Accounting and Supply Control of COMSEC Material. This is the COMSEC custodian's primary reference. It provides information on safeguarding, accounting and reporting procedures, protecting material, and supply procedures. It applies the policy of AR 380-40. When there is a conflict between this technical bulletin and other DA publications on the procedures for safeguarding, accounting, and supply control of COMSEC material, the procedures of TB 380-41 shall be used.

7. Summary. COMSEC material must be protected. To effectively provide protection, a variety of designators and protective markings are used. Coupled with a separate and distinct accountability system, they permit the COMSEC custodian to enforce security.

LESSON 3

PRACTICE EXERCISE

The following items will test your grasp of the material covered in this lesson. There is only one correct answer for each item. When you complete the exercise check your answers with the answer key that follows. If you answer any item incorrectly, study again that part of the lesson which contains the portion involved.

1. What does the term key mean?

   A. The system of physical restraints to unauthorized entry or access

   B. The sequence of randomly-generated binary bits used for encrypting or decrypting signals

   C. The cipher lock system used for facility access

   D. Signal operation instructions

2. What are the four major types of COMSEC keys?

   A. Sargent/Greenleaf, American, Master, and Dibold

   B. One-time pad, signal operation instructions (SOI), Communications-Electronics Operation Instructions (CEOI), and standing operating procedures (SOP)

   C. Traffic encryption, key encryption, transmission security, and key production

   D. Traffic encryption, traffic decryption, key encryption, and key decryption

3. What is FOUO?

   A. A protective marking for information for official use only (not for public disclosure)

   B. A classification marking for material which, if disclosed, could cause serious harm to national interests

   C. A classification marking for information for official use only (not for public disclosure)

   D. An obsolete administrative marking

4. What is the primary reference a COMSEC custodian should have?

   A. AR 380-20

   B. AR 200-10

   C. AR 380-40

   D. TB 380-41 series

5. To what does ARKAG 2 refer?

   A. COMSEC classification guide

   B. COMSEC material control system

   C. Army COMSEC administrative group

   D. COMSEC Material Management Data Catalog

6. To what does CIIC refer?

   A. COMSEC internal inventory code

   B. Controlled item inventory code

   C. Counter-intelligence investigation code

   D. Communications intercept code

7. What is the major reference for COMSEC information about accounting and reporting procedures?

   A. TB 380-41 series

   B. AR 380-5

   C. AR 380-19

   D. FM 380-5

LESSON 3

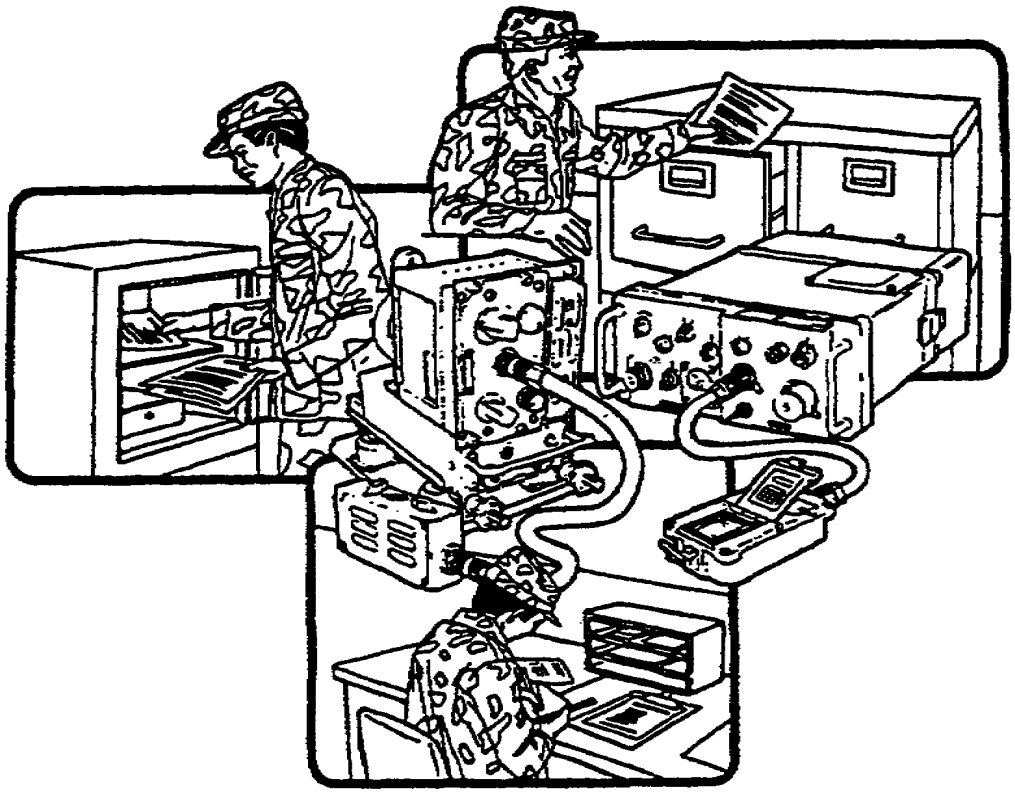
PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

Item	Correct Answer and Feedback	
1.	B.	The sequence of randomly-generated binary bits used for encrypting or decrypting signals The term key means the sequence of randomly-generated binary bits used for encrypting or decrypting signals (page 3-2, para 2a).
2.	C.	Traffic encryption, key encryption, transmission security, and key production The four major types of COMSEC keys are traffic encryption, key encryption, transmission security, and key production (page 3-2, para 2a(1-4)).
3.	A.	A protective marking for information for official use only (not for public disclosure) FOR OFFICIAL USE ONLY (FOUO) is a protective marking for information for official use only (not for public disclosure)(page 3-4, para 5b).
4.	D.	TB 380-41 series The TB 380-41 series is the primary reference a COMSEC custodian should have (page 3-5, para 6d).
5.	D.	COMSEC Material Management Data Catalog ARKAG 2 refers to the COMSEC Material Management Data Catalog (page 3-3, para 4).
6.	B.	Controlled item inventory code CIIC refers the controlled item inventory code (page 3-3, para 4b).
7.	A.	TB 380-41 series The TB 380-41 series is the primary reference for COMSEC information about accounting and reporting procedures (page 3-5, para 6d).

LESSON 4

ACCOUNTABILITY WITHIN THE COMSEC MATERIAL CONTROL SYSTEM



FOR OFFICIAL USE ONLY

LESSON 4

ACCOUNTABILITY WITHIN THE COMSEC MATERIAL CONTROL SYSTEM

CRITICAL TASKS: 01-5770.07-9001
01-5879.07-9001

OVERVIEW

LESSON DESCRIPTION:

In this lesson, you will learn about COMSEC material control. You will also learn about related accounting codes and the controls used with those codes.

TERMINAL LEARNING OBJECTIVE:

ACTION: Describe the categories of the ALC's and how they are used to control COMSEC material.

CONDITION: Given this lesson.

STANDARD: To demonstrate competence, you must achieve a minimum of 70 percent on the subcourse examination.

REFERENCES: The material in this lesson was derived from the following publications: JCS Pub 1-04, AR 380-5, AR 710-2, and TB 380-41 series.

INTRODUCTION

Due to the sensitivity of COMSEC material, there are distinct accounting and reporting procedures. Various Army activities are charged with the accountability of COMSEC material. They are meticulous in how they monitor the status of COMSEC equipment and related keying material. As a signal officer, your COMSEC-related duties normally center on the COMSEC account. When you handle COMSEC material, you must know that accuracy is of the utmost concern. Your account is subject to an audit at any time. You must keep accurate records and always be prepared to have them reviewed.

1. General. The Army CMCS was set up to account for centrally accountable COMSEC material.

a. COMSEC accountability is the job of the officially designated custodian of a COMSEC account or subaccount. The custodian maintains formal records of accountable COMSEC material to provide proper security, accounting, and reporting. Accounting procedures provide for the positive and continuous control of COMSEC material. This occurs from time of receipt through authorized and documented destruction or final disposition.

b. The CCSLA develops and issues approved COMSEC accounting procedures. It also conducts audits of COMSEC accounts and manages the CMCS. The CMCS includes the ACCOR.

c. The ACCOR maintains a continuous and exact record of Army material. The ACCOR is the principal Army activity charged with maintaining records of centrally accountable COMSEC material.

d. The Department of the Army establishes a COMSEC field office of record (CFOR) during contingency conditions or a state of hostile conflict. The CFOR assumes ACCOR responsibilities for all COMSEC accounts within the theater of operation. Procedures directing the COMSEC custodian to report to the ACCOR are understood to mean the COMSEC custodian reports directly to CFOR during the CFOR's existence. A CFOR reports COMSEC account information for its theater of operations directly to the ACCOR. It does this on a consolidated basis for updating the Army master inventory.

e. COMSEC logistics is the Army system for acquiring, storing, moving, distributing, securing, accounting, maintaining, and disposing of COMSEC material. It supplements, but does not replace, the Army logistics systems. The CLSFs provide COMSEC logistic support. They include:

(1) COMSEC logistic support centers (CLSC). A CLSC provides COMSEC logistics support to a field Army or equivalent force. It provides support to other activities as directed.

(2) COMSEC logistic support units (CLSU). A CLSU provides COMSEC logistics support to a corps or on a geographical basis.

(3) COMSEC material direct support activities (CMDSA). A CMDSA is an element of a unit or an organization that provides the COMSEC office of record materiel support. It also provides maintenance support, if authorized.

(4) COMSEC servicing accounts (CSA). A CSA supports Army Reserve and National Guard accounts and subaccounts.

f. The ACCLAIMS is a computer system that provides automatic data processing support to COMSEC accounts. Only the CCSLA can approve deviations or exceptions to set policies and procedures.

(1) It allows a custodian to automatically issue or transfer keying material by short title.

(2) It allows a custodian to maintain COMSEC holdings of subaccounts and hand receipt holders.

(3) It prints a listing of holdings for subaccounts/hand receipt holders.

(4) When used, ACCLAIMS ends the need for DA Form 2008, DA Form 2009, DA Form 2011, DA Form 2011-1, and DA Form 4669-R.

(5) There are four levels within ACCLAIMS.

(a) Level 1-CCSLA.

(b) Level 2-Blue Grass Army Depot.

(c) Level 3-Theater CLSC, Europe.

(d) Level 4-User COMSEC accounts.

g. The CMCS uses the numeric ALC to show the minimum accounting controls needed for COMSEC material. The ARKAG 2 lists these ALCs. The ARKAG 2 is a master listing of all Army COMSEC material.

2. COMSEC accounts.

a. TB 380-41 series, Procedures for Safeguarding, Accounting and Supply Control of COMSEC Material, contains procedures used to account for COMSEC material.

b. AR 710-2, Supply Policy Below the Wholesale Level, describes using unit property books. Army classified COMSEC equipment is identified in the unit property book. However, that inclusion only reflects authorization and identification data. The TB 380-41 series contains specific data on the terminology and limitations involved in this accounting.

c. The materiel management policies in AR 710-2 are followed, except when COMSEC is specifically exempted.

d. User accounts are COMSEC accounts that have been set up solely to manage organic COMSEC equipment. User accounts do not have specified supply or maintenance support missions. AR 710-2 is the supply guide for such accounts.

e. COMSEC accounts that have been given specified supply or maintenance missions in support of organic or nonorganic customers are COMSEC support activities. AR 710-2 is also used for these accounts.

f. Accountable COMSEC material includes all COMSEC keying material, publications, and classified equipment and components. Accountable COMSEC material is assigned an ALC and is controlled in the CMCS.

3. Administration. Direct communication of routine COMSEC accounting activities is authorized between those accounts reporting to the ACCOR and that office. Routine COMSEC accounting communications are addressed to Commander, CCSLA (ATTN: SELCL-KPD-OR). Refer to the TB 380-41 series for specific address information.

4. COMSEC material accounting legend codes. The ALC is a numeric code assigned to COMSEC material. It indicates the degree of accounting and control needed for that piece of material. The CCSLA can upgrade an ALC, but only the NSA can downgrade one. The COMSEC custodian uses the ARKAG 2 to obtain or verify the ALC for all COMSEC material in his account. He also uses the ARKAG 2 to verify the correct short title of COMSEC material. COMSEC material is assigned an ALC of 1, 2, 3, or 4.

a. COMSEC accounts.

(1) ALC 1 material is accountable to the ACCOR by serial number.

(2) ALC 2 material is accountable to the ACCOR by quantity.

(3) ALC 3 material is accountable to the ACCOR by serial number for only major distribution accounts. User account and CMDSAs account for ALC 3 locally until final disposition.

(4) ALC 4 material is not accountable to the ACCOR. However, the COMSEC custodian accounts for his material locally until final disposition. There are no accounting requirements for unclassified, non-crypto marked ALC 4 material.

b. COMSEC subaccounts.

(1) ALC 1 material is accountable to a CMDSA by serial number.

(2) ALC 2 material is accountable to a CMDSA by quantity.

(3) ALC 3 and ALC 4 material is not accountable to a CMDSA. However, the subaccount custodian accounts for the material locally until final disposition.

5. Summary. Effective security begins with accountability. The heart of the COMSEC system is its need to maintain positive and continuous accountability. This occurs from point of origin to final disposition. As a signal officer with COMSEC related duties, you must be totally conversant in all aspects of the CMCS. You must know the ALCs and the degree of accounting and control needed.

LESSON 4

PRACTICE EXERCISE

The following items will test your grasp of the material covered in this lesson. There is only one correct answer for each item. When you complete the exercise, check your answers with the answer key that follows. If you answer any item incorrectly, study again that part of the lesson which contains the portion involved.

1. A maneuver battalion has a COMSEC facility. Who is responsible for COMSEC material accountability?

   A. The unit supply officer

   B. The COMSEC custodian

   C. The COMSEC alternate custodian

   D. The unit signal officer

2. Which of the following best describes ACCLAIMS?

   A. A product improvement program established by the CCSLA

   B. A computer system that provides automatic data processing support to COMSEC accounts

   C. An accountability program for COMSEC subaccounts

   D. A computer system used by the Army National Guard

3. Where are accounting legend codes found?

   A. Appropriate Table of Organization and Equipment/Table of Distribution and Allowances (TOE/TDA)

   B. TB 340-81

   C. ARKAG 2

   D. AR 710-2

4. For a COMSEC account, what does an ALC 1 indicate about the COMSEC material?

   A. Accountable to the ACCOR by serial number

   B. Accountable to a CMDSA by serial number

   C. Accountable to both the ACCOR and a CMDSA by serial number

   D. Accountable to the ACCOR by quantity

5. For a COMSEC subaccount, an ALC 2 indicates the material is accountable to which of the following?

   A. The ACCOR by quantity

   B. A CMDSA by serial number

   C. A CMDSA by quantity

   D. The ACCOR by serial number

6. What does an ALC 4 in a COMSEC subaccount indicate?

   A. The material is accountable to the ACCOR by serial number

   B. The material is accountable to a CMDSA by quantity

   C. The material is not accountable to a CMDSA

   D. The material is accountable to the ACCOR by quantity and to a CMDSA by serial number

LESSON 4

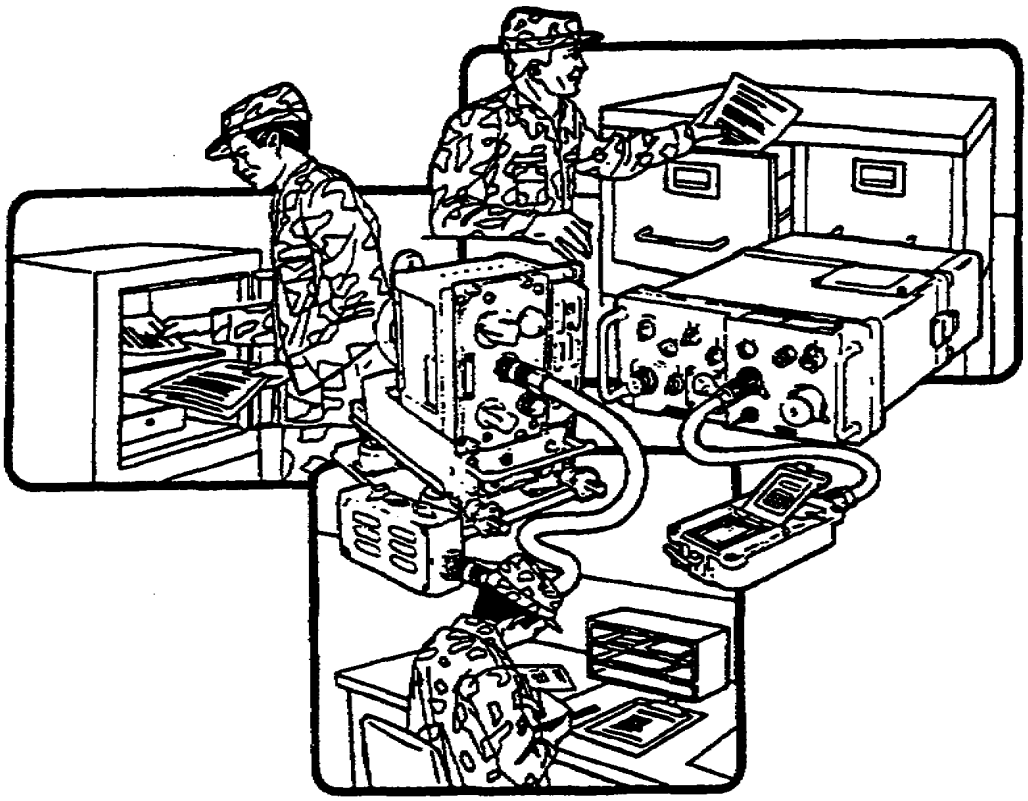
PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

Item	Correct Answer and Feedback
1.	B. The COMSEC custodian The COMSEC custodian is responsible for COMSEC material accountability in a maneuver battalion that has a COMSEC facility (page 4-2, para 1a).
2.	B. A computer system that provides automatic data processing support to COMSEC accounts ACCLAIMS is a computer system that provides automatic data processing support to COMSEC accounts (page 4-3, para 1).
3.	C. ARKAG 2 Accounting legend codes are found in the COMSEC Material Management Data Catalog (ARKAG 2) (page 4-4, para 4).
4.	A. Accountable to the ACCOR by serial number For a COMSEC account, an ALC 1 indicates that the COMSEC material is accountable to the ACCOR by serial number (page 4-4, para 4a(1)).
5.	C. A CMDSA by quantity For a COMSEC subaccount, an ALC 2 indicates the material is accountable by quantity to a CMDSA (page 4-4, para 4b(2)).
6.	C. The material is not accountable to a CMDSA An ALC 4 in a COMSEC subaccount indicates the material is not accountable to a CMDSA (page 4-4, para 4b(3)).

LESSON 5

PHYSICAL SECURITY FOR COMMUNICATIONS SECURITY



FOR OFFICIAL USE ONLY

LESSON 5

PHYSICAL SECURITY FOR COMMUNICATIONS SECURITY

CRITICAL TASKS: 01-5770.07-9001
01-5879.07-9901

OVERVIEW

LESSON DESCRIPTION:

In this lesson, you will learn about the requirements for COMSEC, physical security, and associated facilities. With this information, you will be able to establish procedures and supervise the proper storage of COMSEC material.

TERMINAL LEARNING OBJECTIVE:

ACTION: State the requirements for protecting a cryptofacility and for the proper storage of COMSEC material.

CONDITION: Given this lesson.

STANDARD: To demonstrate competence, you must achieve a minimum of 70 percent on the subcourse examination.

REFERENCES: The material in this lesson was derived from the following publications: AR 190-13, AR 380-5, AR 380-19, AR 380-19-1, AR 380-40, FM 19-30, and TB 380-41 series.

INTRODUCTION

This lesson covers the basic procedures for safeguarding COMSEC material and associated facilities. These procedures ensure the integrity of COMSEC material. They address many threats to COMSEC. Some of these are loss, theft, sabotage, and unauthorized access to COMSEC material. Other threats include tampering with and the clandestine exploiting of sensitive communications within a secure facility.

1. General. The three types of cryptofacilities (hereafter referred to as facilities) are fixed, mobile, and transportable. These facilities present different physical security challenges.

a. A fixed facility is vulnerable to both overt and covert attempts to gain access to it and its contents. The standards to be met in constructing a facility and controlling access are in several Army regulations AR 190-13, AR 380-5, AR 380-19-1, and AR 380-40). There are a variety of security requirements to meet. The following are general guidelines:

(1) The facility is located in a secure room or controlled area.

(2) The commander enforces facility access regulations when the facility is used for general office purposes.

(3) The facility is located in a building of substantial construction. Entry-resistant and opaque materials are used.

(4) Needed openings (windows, peepholes, and vents) are covered to prevent unauthorized access or observation of operations.

(5) The facility has a single door that is used for both entry and exit. There may be emergency exit doors, but they are secured to prevent unauthorized entry. Those exits use a deadbolt emergency exit device with a local alarm.

(6) Personal equipment capable of receiving, transmitting, recording, or amplifying emissions cannot be brought into the facility. These include cameras, radios, tape recorders, and televisions. Only government-owned items directly associated with COMSEC operations are allowed in the facility.

(7) Electronic control devices cannot substitute for the required combination lock for the facility. Control devices (cipher locks, keyless pushbuttons, and so forth) may be used with the required combination lock. These devices may be used only for admitting authorized persons to an occupied or guarded facility. Cipher locks and keyless pushbuttons are conveniences. They are not used for control or security.

b. The requirements for securing mobile and transportable facilities are about the same. The principles that apply to fixed facilities apply equally to mobile and transportable facilities.

(1) All transportable and mobile facilities are protected by guards.

(2) The operators can serve as guards. This applies when the facility layout and operator duties make it feasible for operators to provide adequate control.

(3) Guards are stationed within sight of the facility when there is no supplemental protection. A physical barrier against entry is one type of supplemental protection. Guards are posted if there is a possibility of unauthorized vehicle removal.

(4) A guard post or a patrol may be used if it is supplemented by an alarm system. The response time for a reaction force should not exceed 5 minutes. If a vehicle is involved, the alarm system must be implemented so there is no possibility of unauthorized vehicle removal.

2. Protecting stored COMSEC material.

a. Storage protects COMSEC material or information when it is not under the direct and continuous control of properly cleared and authorized personnel. Some storage methods are security containers and vaults. They may be supplemented by alarms and guards. The protection of classified COMSEC material is presumed when it is used by, in the physical possession of, or continuously attended by properly cleared personnel. Different security standards are needed for the different classification levels involved. These levels are TOP SECRET, SECRET, and CONFIDENTIAL.

(1) TOP SECRET material is stored in a GSA approved safe-type security file cabinet. It may also be stored in a Class A vault or in an alarm-equipped or guarded area.

(2) SECRET material may be stored by any of the TOP SECRET storage methods noted above. Other methods are a GSA-approved steel file with a built-in, three-position, dial-type combination lock, or a Class B vault.

(3) CONFIDENTIAL material may be stored by any of the TOP SECRET or SECRET storage methods noted above. It may also be stored in a steel file cabinet with a built-in, changeable, three-position combination lock.

(4) UNCLASSIFIED CRYPTO key is stored using the same methods used for classified key, if practicable. It may also be stored in the most secure manner available to the user.

b. COMSEC equipment and components are in either an operational or a nonoperational configuration. The following are differences in storage requirements:

(1) Nonoperational.

(a) These unkeyed items are stored in the same manner set forth for material of the same classification.

(b) Unclassified equipment and components will be stored by a suitable method that prevents any reasonable possibility of theft, tampering, or access by unauthorized personnel. This does not apply to CCI. Normally, the same protection provided for vehicles, or high value and pilferable government property, is adequate for

protecting unkeyed COMSEC equipment installed in vehicles and facilities. The commander considers all aspect of the property and the environment when deciding acceptable security needs and methods for protecting unkeyed COMSEC equipment.

(2) Operational.

(a) Unkeyed classified COMSEC equipment may be installed in an operational configuration in a ship, aircraft, vehicle, building, and so forth. When so installed, it may be left unattended. This applies only when it is protected to the degree the commander believes sufficient to prevent the likelihood of theft, sabotage, tampering, or access by unauthorized persons.

(b) Where the installed COMSEC equipment is keyed, the provisions of paragraphs 2a and 2b related to storage apply. This is according to the classification of the equipment and its key.

(c) Installed COMSEC equipment will not be removed from a vehicle for the sole purpose of providing security. Frequent removal and reinstallation of COMSEC equipment causes equipment failure and reduces operational readiness.

c. Only limited amounts of essential keying material may be stored in a mobile facility.

(1) The requirement for storage containers and guards, noted above, applies. This is based on the classification of the cryptomaterial.

(2) Security containers are securely affixed to the facility.

(3) No more than a single edition of keying material is held.

(4) COMSEC holdings are limited to those essential to mission performance.

(5) Unattended mobile facilities containing keying material or keyed COMSEC equipment are guarded by cleared personnel.

3. Using COMSEC equipment at unattended sites. The cryptomaterials and cryptokeys used to protect communications are the key to secure communications. However, as U.S. forces cooperate more with forces of other nations, certain COMSEC equipment may have to be located at unattended sites. Safeguards must be in effect for the security of COMSEC equipment at unattended sites.

a. The site must be located in an area under either U.S. or allied control.

b. Adequate U.S. or allied forces must be located in the vicinity of any unattended site. The force must be sufficient enough to prevent the possibility of enemy capture or temporary occupation of that site.

c. Uninstalled spare equipment cannot be at unattended sites. Only one on-line spare may be installed for available circuits.

d. Keying material other than that electrically or physically held in the COMSEC equipment cannot be stored at an unattended site.

e. Unattended sites must be inspected periodically, but no less-than once a month. The purpose is to verify that no one has tampered with the COMSEC equipment.

4. Summary.

a. The three types of cryptofacilities are fixed, mobile, and transportable.

b. A facility must meet the physical security requirements established by Army regulations. These include:

(1) The structural integrity of the facility.

(2) Substantial safes and cabinets used to store COMSEC material.

c. The soldier is the most important link in protecting COMSEC material.

LESSON 5

PRACTICE EXERCISE

The following items will test your grasp of the material covered in this lesson. There is only one correct answer for each item. When you complete the exercise, check your answers with the answer key that follows. If you answer any item incorrectly, study again that part of the lesson which contains the portion involved.

1. What are the three types of cryptofacilities?

   A. Non-fixed, mobile, and transportable

   B. Fixed, mobile, and transportable

   C. Fixed, mobile, and non-transportable

   D. Fixed, non-mobile, and transportable

2. Which items are permitted in a cryptofacility?

   A. Personal radios and television sets

   B. Personal cameras that are empty

   C. Any government-owned item or item of government issue

   D. Government-owned items directly related to the facility

3. Protecting a mobile facility requires which of the following?

   A. Full-time guards, regardless of whether or not operators are present

   B. Guards, although the operators can serve as guards

   C. Guard posts or roving patrols within 100 meters of the facility

   D. Personnel who serve only as guards, without exception

4. On what are the different standards of security for protecting stored COMSEC material based?

A. The different levels of classification involved

B. The amount of crypto equipment being stored

C. The type of facility

D. Operational conditions on the battlefield

5. Keying material is stored in a mobile facility. Which of the following applies?

A. Storage containers must be approved to meet the appropriate classification level

B. Up to three editions of the keying material may be held

C. No keying material may be held in mobile storage

D. COMSEC items essential to ongoing operations cannot be stored in a mobile facility

6. Safeguards must be followed for the security of COMSEC equipment at unattended sites. Which of the following describes them?

A. They do not exist because COMSEC equipment cannot be at an unattended site

B. They include the need for the site to be under U.S. control only

C. They include the need for the site to be under either U.S. or allied control

D. They do not include the need for periodic inspections

LESSON 5

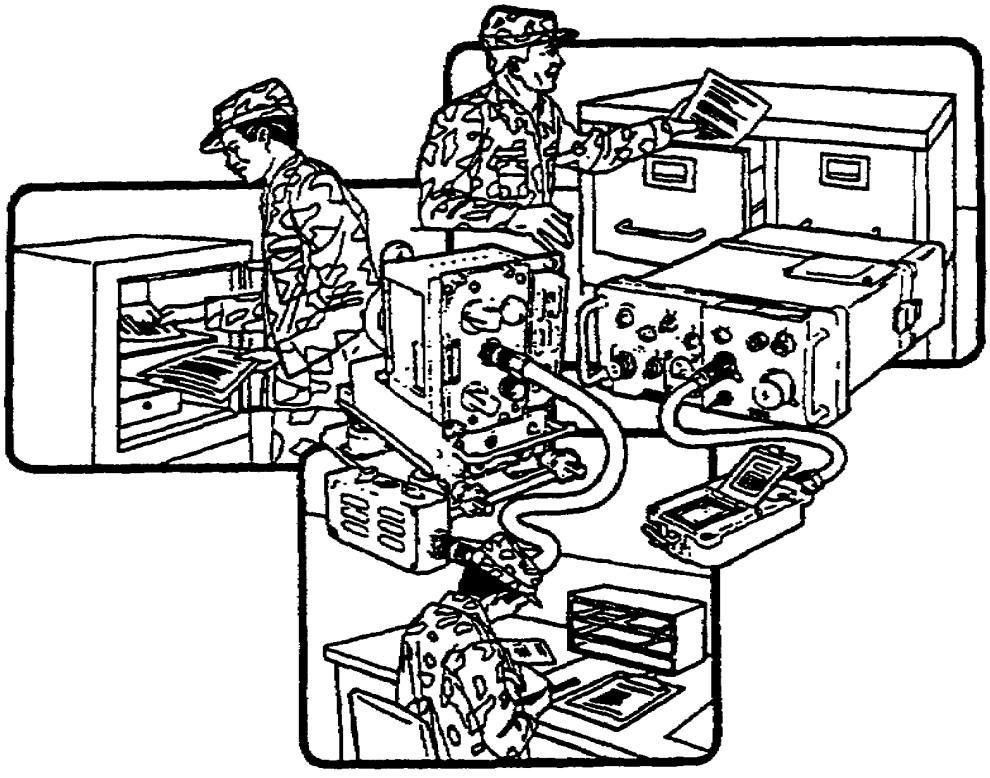
PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

Item	Correct Answer and Feedback	
1.	B.	Fixed, mobile, and transportable The three types of cryptofacilities are fixed, mobile, and transportable (page 5-2, para 1).
2.	D.	Government-owned items directly related to the facility Government-owned items directly related to the facility are permitted in a facility (page 5-2, para 1a(6)).
3.	B.	Guards, although the operators can serve as guards Protecting a mobile facility requires guards. However, the operators can serve as guards (page 5-2, para 1b (2))
4.	A.	The different levels of classification involved The different standards of security for protecting stored COMSEC material are based on the different levels of classification involved (page 5-3, para 2a).
5.	A.	Storage containers must be approved to meet the appropriate classification level When keying material is stored in a mobile facility, the storage containers must be approved to meet the appropriate classification level (page 5-4, para 2c(1)).
6.	C.	They include the need for the site to be under either U.S. or allied control Safeguards for the security of COMSEC equipment at unattended sites include the need for the site to be under either U.S. or allied control (page 5-4, para 3b).

LESSON 6

COMMUNICATIONS SECURITY
EMERGENCY PLANS



FOR OFFICIAL USE ONLY

LESSON 6

COMMUNICATIONS SECURITY EMERGENCY PLANS

CRITICAL TASKS: 01-5770.07-9001
01-5879.07-9001

OVERVIEW

LESSON DESCRIPTION:

In this lesson, you will learn about the importance of preparing adequate emergency plans for COMSEC material. You also will learn about practicing and executing procedures for securely storing, destroying, and evacuating COMSEC material.

TERMINAL LEARNING OBJECTIVE:

ACTION: Describe the content of cryptofacility emergency plans and state the procedures for preparing, practicing, and executing them.

CONDITION: Given this lesson.

STANDARD: To demonstrate competence, you must achieve a minimum of 70 percent on the subcourse examination.

REFERENCES: The material in this lesson was derived from the following publications: AR 380-5, AR 380-19, AR 380-40, and TB 380-41 series.

INTRODUCTION

Cryptosecurity material is vital to ensure secure command, control, and communications. However, unplanned events occur on and off the battlefield. These include tornadoes, terrorist attacks, civil uprisings, and surprise enemy attacks. They represent real threats to COMSEC material. COMSEC custodians are responsible for preparing emergency plans that can be implemented, regardless of the emergency. They must know how to plan, prepare, and implement emergency plans. The signal officer must ensure they can do these tasks.

1. General. Commanders must safeguard COMSEC material in the event of natural disasters and hostile actions. The COMSEC custodian is the one who prepares the emergency plans. These plans must be realistic, simple, and workable.

a. For natural or man-made disasters, planning focuses on using or safely storing the material until order is restored. These disasters include fire, flood, tornado, and earthquake. The planning effort provides for:

(1) Fire reporting and initial fire fighting by personnel on duty at a fixed or mobile facility.

(2) Assigning on-the-scene responsibility for controlling access to the facility and COMSEC material. This applies when outside personnel or uncleared emergency crews are admitted to the facility.

(3) Securing or removing COMSEC material and evacuating the area.

(4) Assessing and reporting probable exposure of COMSEC material to unauthorized persons during an actual emergency.

(5) Post-emergency inventory of COMSEC material. This includes reporting any losses or unauthorized exposures.

b. Planning for hostile action centers on procedures to effectively evacuate, secure, or destroy COMSEC material. Hostile actions include a mob action, a civil uprising, or an enemy or terrorist attack on a facility. These plans address the variety of situations that might occur. Emergency plans must cover various situations. These include the facility being overrun by an enemy, or an unstable political environment where destruction must be done immediately. The planning provides for:

(1) The availability and adequacy of physical protective measures. These include perimeter controls and physical security provisions for facilities.

(2) The security procedures and assets needed to evacuate COMSEC material under emergency conditions.

(3) The destruction facilities and assets needed to effectively destroy COMSEC material.

c. Frequent training exercises should be conducted. These ensure personnel know what their tasks and responsibilities are in securing or destroying COMSEC material. Only through rehearsed training exercises can the commander the COMSEC custodian, and other individuals decide if the plans are realistic, simple, and workable.

d. Records of the training exercises are kept with the emergency plans. The COMSEC custodian prepares a record for each exercise. The record notes the training date, the plans tested, the result, and the names of participants.

2. Emergency plan. Planning must begin before an emergency occurs. Thorough planning is vital to have effective emergency procedures. When appropriate, the COMSEC custodian includes the following in his emergency plans:

a. Clear authorization for the senior member present at the time of an emergency to start the plan.

b. Designation of specific duties and responsibilities by duty position, rather than by name. Alternates are also designated.

c. The location of combinations to containers of COMSEC material.

d. The location of COMSEC material, by storage container.

e. Instructions for removing accounting records. These include hand receipt to help the post-emergency inventory. Do not destroy the accountability records.

f. Clear designation of the evacuation and at least one alternate site. The primary and alternate routes of travel are included.

g. The location of fire fighting equipment.

h. Instructions for admitting uncleared emergency personnel (such as firemen) to the facility. Instructions for safeguarding the COMSEC material during such access are included.

i. Provisions for packing, loading, transporting, and safeguarding COMSEC material during transit.

j. Provisions for removing and storing the key and the card reader insert board (if applicable) from equipment when emergency storage is carried out.

k. The location of items to be used to destroy crypto equipment and material.

l. Provisions for those actions taken as a precaution, pending possible destruction.

m. An annual review of the emergency plan and assigned duties by all personnel.

n. The schedule for unannounced simulated emergency training exercises.

o. The reporting instructions.

p. Instructions for storing classified material in accordance with the level of classification involved.

3. Coordination. Planning cannot be done in a vacuum. Planning for emergency situations must be coordinated and made part of the command emergency plan package. The COMSEC custodian, the signal officer, and the operations officer do this coordination.

4. Emergency measures. The three measures a commander can take in an emergency are evacuation, secure storage, or destruction. Carefully consider evacuation or secure storage before resorting to destruction. However, conditions may cause the simultaneous implementation of any two or all three measures to be appropriate. Occasions can arise (such as short-term civil disturbance) where the superseded key will be destroyed, the future key evacuated, and the equipment securely stored. A key word in developing emergency plans and associated actions is anticipate. If an emergency is imminent, reduce on-hand COMSEC material to a minimum. This anticipation reduces the amount of material that must be stored, evacuated, or destroyed.

5. Emergency evacuation. This is removing COMSEC material to a safe, alternate location. It is carried out in a systematic manner and under the direction of a responsible individual.

a. When conducting an emergency evacuation, make every effort to prevent loss or unauthorized access. This is done from the start of the evacuation and ends with the eventual return to the original location or another facility.

b. There are many factors to consider before deciding to evacuate COMSEC material during a emergency. Some of these factors are:

(1) The time available.

(2) Future requirements for the COMSEC material involved.

(3) The degree of hazard involved in removing and evacuating the COMSEC material.

(4) The safety of the new location.

(5) The available means of transportation and evacuation.

(6) The available transportation and evacuation routes.

6. Emergency storage Selecting emergency storage presupposes returning to the site. It also assumes the storage facilities will be sufficient to safeguard the COMSEC material. Storage facilities include authorized vaults, safes, or secure rooms. If secure rooms are used, classified boards must be removed from nonsecured COMSEC equipment. They are stored in approved security containers. The factors to consider include:

a. The time available.

b. The nature of the emergency; that is, whether it is of human origin or natural causes.

c. The seriousness of the emergency.

d. The capability and availability of logistical support. The material's bulk and weight are the primary factors to consider.

e. Emergency storage. This is not an option when under the threat of an enemy attack. In this situation the necessary destruction plan is begun.

7. Emergency destruction. The commander selects emergency destruction for a facility. His decision is based on a comprehensive threat assessment, the facility's condition, and available destruction facilities. The three major areas of interest in emergency destruction are the priorities, the methods, and the destruction records.

a. There are nine priorities of cryptomaterial destruction. These priorities are listed in descending order of importance.

(1) Superseded and current classified keying material marked CRYPTO. These are given the highest destruction priority.

(2) Superseded, current, and future card reader insert boards (CRIB).

(3) TOP SECRET multiholder key that becomes effective within the next 30 days.

(4) Superseded tactical operations codes.

(5) SECRET and CONFIDENTIAL multiholder key that becomes effective within the next 30 days.

(6) Sensitive pages of crypto equipment manuals or the complete manual.

(7) CLASSIFIED elements or subassemblies of COMSEC equipment in the order listed in the maintenance manuals.

(8) The balance of COMSEC equipment maintenance manuals and classified operating instructions.

(9) Any remaining classified COMSEC material and unclassified keying material marked CRYPTO. Superseded authenticators and unused two-copy (point-to-point) key are destroyed if time permits.

b. Destruction must render COMSEC equipment unusable and nonrepairable. The means and methods to do this vary, depending on what is being destroyed.

(1) Key and COMSEC documents are destroyed as the commander specifies. Devices or methods approved for routine destruction are acceptable, if the device or method used will totally destroy the material. The following can be used to destroy documents:

(a) Shredders.

(b) Document destroyer kits.

(c) Incendiary file destroyer.

(d) Fuels.

(2) COMSEC equipment, as a general guideline, is only destroyed as a last resort to prevent it from falling into unauthorized hands. Its destruction must be thorough enough to destroy all logic circuits. If the classified assemblies are destroyed, the remainder of the equipment does not have to be destroyed. The following are approved for emergency destruction:

(a) Thermite incendiaries.

(b) Incinerators.

(c) Fire axes.

(d) Acetylene torches.

(e) Whenever emergency plans are used, message reports are sent to several addressees. A copy is sent to the Intelligence and Security Command. Another copy is sent to the Communications Security Logistics Activity. The COMSEC supporting elements within the chain of command also receive a copy. TB 380-41 contains the addresses.

(3) If an emergency incident does not result in a security violation, the report will:

(a) List the material destroyed or relocated.

(b) State the method and degree of destruction.

(c) State the circumstances that caused the emergency plans to be used.

(4) If an emergency incident results in a security violation, four separate reports are sent.

(a) The initial report provides all available facts about the destruction or abandonment of COMSEC material.

(b) The amplifying report provides significant new information about the incident, as it is gained.

(c) An Interim report updates the status of the security violation investigation.

(d) The final report deals with the facts and evidence about the reported security violation.

8. Emergency task cards. These are used to prepare and execute emergency plans. They are a logical extension of the basic emergency plan. Each individual card lists a separate task, its priority, and the approximate completion time. The commander ensures these cards are prepared and used. The following are specific about these cards:

a. Identify and record each specific task on a separate card. Record the time for completing each task. Arrange the completed cards in priority order as specified in the emergency plan.

b. In an emergency, personnel report to a predesignated location. There, the COMSEC custodian or other person issues the tasks in priority order.

c. Each individual carries out his assigned task. He reports back to the officer in charge when his task has been completed. This way, the COMSEC custodian is aware of which tasks have been completed, are underway, or need to be initiated. This procedure continues until all tasks are completed.

d. A facility may have multiple emergency plan taskings and responsibilities. Thus, the emergency task card function may be completed within Individual sections.

9. Summary. Planning for COMSEC emergencies cannot wait until an emergency is imminent or underway. Prudent security measures require preparing and testing of plans to protect COMSEC material. These plans include evacuation, emergency storage, and destruction. As these plans are carried out, care must be taken to ensure unauthorized access to equipment and material does not occur.

LESSON 6

PRACTICE EXERCISE

The following items will test your grasp of the material covered in this lesson. There is only one correct answer for each item. When you complete the exercise, check your answers with the answer key that follows. If you answer any item incorrectly, study again that part of the lesson which contains the portion involved.

1. Commanders consider which of the following when planning for natural disasters?

   A. Post-emergency inventory of COMSEC material

   B. In the event of natural or man-made disasters, there is no way to properly plan for such unforeseen occurrences

   C. The probability of such events is extremely low; therefore, planning for such events has little return

   D. The post Directorate of Security will assume all responsibility for COMSEC material

2. What should you focus on when planning for natural disasters?

   A. The evacuation and controlled destruction of COMSEC material

   B. The evacuation of assigned or attached personnel from the facility

   C. The use or safe storage of COMSEC material until order is restored

   D. The reporting procedures to be followed after the emergency is over

3. What does COMSEC emergency planning involve?

   A. Planning only

   B. Planning and conducting training exercises based on emergency plans

   C. Planning and conducting training exercises and keeping records of training exercises

   D. Planning and preparing reports associated with emergency destruction

4. Emergency plans contain classified material. Which of the following describes those plans?

   A. They must be kept in open storage, so they are immediately available in an emergency

   B. They may be kept in whatever storage the commander wants

   C. They must be kept in the most secure storage available, regardless of the level of classification involved

   D. They must be securely stored in accordance with the level of classification involved

5. When is emergency storage not an option?

   A. When your unit is under the threat of an enemy attack

   B. When your unit is under the threat of a local civil riot

   C. When your unit is under the threat of a hurricane

   D. When your unit is under the threat of fire within the facility

6. Which of the following describes emergency task cards?

   A. They are required for all emergency plans

   B. They identify individual tasks, the amount of time required, and the priority

   C. They identify, by name, the individual responsible for each task

   D. They are forwarded through the chain of command to INSCOM with the report of each COMSEC insecurity

LESSON 6

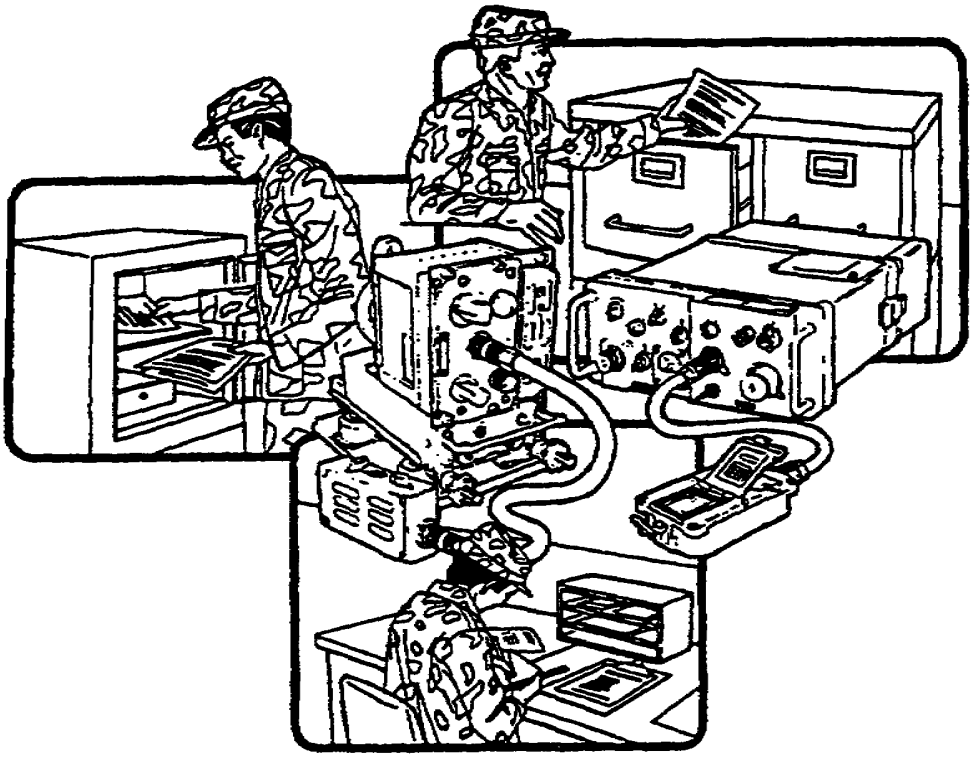
PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

Item	Correct Answer and Feedback
1.	A. Post-emergency inventory of COMSEC material Commanders must consider post-emergency inventory of COMSEC material when planning for natural disasters (page 6-2, para 1a(5)).
2.	C. The use or safe storage of COMSEC material until order is restored The focus should be on the use or safe storage of COMSEC material until order is restored when planning for natural disasters (page 6-2, para 1a).
3.	C. Planning and conducting training exercises and keeping records of training exercises COMSEC emergency planning involves planning, conducting training exercises, and keeping records of training exercises (page 6-2, para 1b-d).
4.	D. They must be securely stored in accordance with the level of classification involved Emergency plans that contain classified material must be securely stored in accordance with the level of classification involved (page 6-3, para 2p).
5.	A. When your unit is under the threat of an enemy attack Emergency storage is not an option when your unit is under the threat of an enemy attack (page 6-5, para 6e).
6.	B. They identify individual tasks, the amount of time required, and the priority Emergency task cards identify individual tasks, the amount of time required, and the priority (page 6-7, para 8a).

LESSON 7

COMMUNICATIONS SECURITY
INSPECTIONS AND AUDITS



FOR OFFICIAL USE ONLY

LESSON 7

COMMUNICATIONS SECURITY INSPECTIONS AND AUDITS

CRITICAL TASKS: 01-5770.07-9001
01-5879.07-9001

OVERVIEW

LESSON DESCRIPTION:

In this lesson, you will learn about the various COMSEC inspections and audits.

TERMINAL LEARNING OBJECTIVE:

ACTION: Describe the purposes and types of COMSEC inspections and the scope of COMSEC audits.

CONDITION: Given this lesson.

STANDARD: To demonstrate competence, you must achieve a minimum of 70 percent on the subcourse examination.

REFERENCES: The material in this lesson was derived from the following publications: AR 190-13, AR 380-5, AR 380-19, AR 380-40, and TB 380-41 series.

INTRODUCTION

The COMSEC custodian is responsible for his account's material. To assist the custodian in his accountability and enhance security by detecting potential COMSEC incidents, the COMSEC system uses a series of inspections and audits. A well-trained custodian, who is conscientious in his duties, knows how to prepare for inspections and audits. He should receive no surprises during the course of the review. Inspectors and custodians use the same regulations in performing their duties.

1. General. The COMSEC custodian and the unit commander should conduct frequent inspections and checks of their cryptofacility. They must ensure that high levels of individual and collective security awareness are maintained.

2. COMSEC account audits.

a. The CCSLA conducts formal audit of COMSEC accounts. These audits involve the physical inventory of all COMSEC material charged to an account. This includes hand-receipted material. They also involve checking accounting records and files and reviewing internal accounting and operating procedures. These audits are conducted separately from INSCOM cryptofacility inspections.

b. Audits are normally scheduled through the responsible command, although they may be unannounced. The CCSLA sets the priority of COMSEC account audit. To do this, it uses the following criteria:

(1) The frequency of custodian changes.

(2) The size, type of account, and number of transactions.

(3) The classification and sensitivity of material held in an account.

(4) Accounting problems noted by the ACCOR.

(5) Physical incidents related to or caused by accounting errors.

(6) Unauthorized absence of a custodian or others holding material on hand receipt.

(7) Requests for audit by the local commander.

(8) INSCOM recommendation.

c. There are five major areas to an audit; however, an audit is not limited to them. The five areas are:

(1) Verifying the completeness and accuracy of all accounting records and files.

(2) Verifying the knowledge of and adherence to COMSEC policy and procedure by the COMSEC custodian and the alternate.

(3) A complete physical inventory of COMSEC material charged to the account, including material on hand receipt.

(4) Soliciting the custodian's accounting problems and making recommendations.

(5) The auditor's recommendations for improving local accounting procedures.

d. After an audit, the CCSLA auditor informs the COMSEC custodian and unit commander of any situation needing immediate action. A formal audit report is sent through command channels to the commander of the audited COMSEC account. This report outlines the COMSEC accounts condition and recommended improvements.

e. The CCSLA recommends that COMSEC material direct support activities conduct local audits of their subaccount. They should use the same approach as CCSLA uses in its audits. Frequency, scope, and reporting of subaccounts should be coordinated with local commands before actual audits.

3. COMSEC inspections. Inspections of COMSEC material are conducted to ensure that COMSEC material is properly protected. Audits of COMSEC accounts will include a total physical inventory of all COMSEC material charged to the account, a check of accounting records and files, and a review of internal accounting and operating procedures.

a. Chapter 6 of AR 380-40, DA Policy for Safeguarding and Controlling COMSEC Information, outlines the conduct of INSCOM and command COMSEC inspections. In addition, frequent inspections or checks of the facility by assigned personnel are strongly recommended.

b. The command inspection is done at the discretion of the responsible commander. Its purpose is to ensure COMSEC material is used, stored, distributed, destroyed, and accounted for according to appropriate rules and regulations. The command inspection system is the backbone of the Army's efforts to ensure COMSEC material receives proper protection.

(1) The interval between command inspections cannot exceed 24 months. However, more frequent inspections are recommended.

(2) Command inspectors are selected, based on their experience and knowledge of COMSEC policies and procedures. Appointed in writing, they must:

(a) Be familiar with AR 380-40 and the TB 380-41 series.

(b) Be a graduate of the Training and Doctrine Command approved Standardized COMSEC Custodian course.

(c) Have had prior experience as a COMSEC custodian or inspector.

(d) Meet the unwaived grade requirements for COMSEC custodian.

(3) The results of a command inspection are recorded on DA Form 2769-R (Cryptofacility Inspection Report). These results are maintained on file until the results of the next command inspection are received. DA Form 2769-R is shown in Figures 7-1 and 7-2.

(4) Discrepancies discovered during the command inspection must be reconciled within 30 days after receipt of the inspection report. A reply by endorsement is forwarded through command channels to the command inspector.

c. An INSCOM responsibility is to provide technical assistance to Army activities having prime COMSEC accounts. To do this, INSCOM conducts inspections of selected critical Army COMSEC accounts. These include subaccounts and hand receipts as needed. However, not all COMSEC custodians can expect a visit from an INSCOM inspection team.

(1) Activities that are subject to an INSCOM inspection include:

(a) COMSEC logistic support facilities.

(b) Key distribution and generation centers.

(c) Selected strategic secure communications facilities.

(d) Direct support, general support, and special repair facilities.

(e) Research, development, test, and evaluation facilities.

(f) Army cryptofacilities servicing defense contractors.

(g) Army communications facilities deployed in high risk areas.

(2) The normal interval of INSCOM inspections is 18 months. INSCOM adjusts this interval as needed. Factors considered in deciding on the inspection frequency include:

(a) The results of recent command and INSCOM inspections.

(b) The type of material held in the account.

(c) The threat within the geographic area of the account.

(d) The number and type of COMSEC incidents occurring since the last inspection.

(e) The training and experience level of the command inspector and the COMSEC custodian.

CRYPTOFACILITY INSPECTION REPORT	For use of this form, see TB 380-41: the proponent agency is AMC	DATE

THRU:	TO:	FROM:

CRYPTOFACILITY DATA

ORGANIZATION UNIT IDENT CODE			COMMANDER *(Name and Grade)* COMSEC CUSTODIAN *(Name and Grade)*
ROOM NUMBER	BUILDING NUMBER	FLOOR NUMBER	ALTERNATE(S) *(Name and Grade)*
NUMBER AND STREET		TELEPHONE NO.	
CITY/POST	STATE/COUNTRY		SUPPORTING COMSEC ACCOUNT NUMBER
HOURS OF OPERATION	CRYPTOSYSTEMS OR CRYPTO-EQUIPMENT HELD		

PRIMARY PURPOSE OF CRYPTOFACILITY *(Check One)*

☐ OPERATIONS ☐ DISTRIBUTION ☐ MAINTENANCE ☐ ADMINISTRATIVE ☐ RDTE ☐ STORAGE

DATE OF INSCOM APPROVAL	DATE OF LAST COMMAND INSP	DATE OF LAST INSCOM INSP	DATE OF THIS INSPECTION

FINDINGS AND RECOMMENDATIONS *(If more space is needed, continue on reverse)*

COMMANDER	SIGNATURE

DA Form 2769-R, 1 Nov 77 EDITION OF 1 NOV 74 IS OBSOLETE.

Figure 7-1. DA Form 2769-R (front).

CRYPTOFACILITY INSPECTOR'S RECORD

TRAVEL TIME	INSPECTION TIME	P & R TIME	TYPED NAME OF INSPECTOR	GRADE

ANSWER SHEET FOR APPENDIX E, TB-380-41-1

QUES-TION NO.	ANSWER			QUES-TION NO.	ANSWER			QUES-TION NO.	ANSWER			QUES-TION NO.	ANSWER			QUES-TION NO.	ANSWER		
	YES	NO	N/A		YES	NO	N/A		YES	NO	N/A		YES	NO	N/A		YES	NO	N/A
1				14				27				40				53			
2				15				28				41				54			
3				16				29				42				55			
4				17				30				43				56			
5				18				31				44				57			
6				19				32				45				58			
7				20				33				46				59			
8				21				34				47				60			
9				22				35				48				61			
10				23				36				49				62			
11				24				37				50				63			
12				25				38				51				64			
13				26				39				52				65			

ADDITIONAL SPACE FOR CONTINUATION

Figure 7-2. DA Form 2769-R (reverse).

(3) AR 380-40 is a basic COMSEC reference. It describes the actions commanders and COMSEC custodians should take before INSCOM inspections. It also describes the inspection notification and inspection points of interest.

4. Summary. Inspections and audits can be uncomfortable experiences. The tension that surrounds an audit or inspection can be reduced by having an aggressive and thorough local self-inspection program. The real objective of the auditors and inspectors is to ensure the COMSEC system's security.

LESSON 7

PRACTICE EXERCISE

The following items will test your grasp of the material covered in this lesson. There is only one correct answer for each item. When you complete the exercise, check your answers with the answer key that follows. If you answer any item incorrectly, study again that part of the lesson which contains the portion involved.

SITUATION: The scenario for this exercise has you assigned as a COMSEC custodian.

1. Upon appointment as a COMSEC custodian, you review the SOP for the cryptofacility. Audits is among the topics. Who conducts formal audits?

   A. Your next higher headquarters

   B. The COMSEC custodian

   C. The ACCOR

   D. The CCSLA

2. The telephone rings. You learn your facility will receive an unannounced audit tomorrow. You hang up the telephone and immediately begin to make plans for the audit. Which of the following will the audit include?

   A. A physical inventory of all of the account's COMSEC material. It will not include hand-receipted material

   B. A review of internal accounting and operating procedures

   C. A partial physical inventory of the account's COMSEC material, but not hand-receipted material

   D. A parallel INSCOM cryptofacility inspection

3. You receive notice of a division-directed command inspection of your facility. It has been 10 months since the last command inspection. Which of the following describes the command inspection?

A. It is the backbone of the Army's efforts to ensure COMSEC material receives proper protection

B. It is conducted by an impartial team with limited COMSEC experience

C. Its focus is only on destruction certificates and records

D. It should be conducted by an individual meeting all qualifications for a COMSEC custodian. But it can be conducted by an individual with grade waivers

4. The results of a command inspection are recorded on which of the following?

A. INSCOM letterhead

B. Message form

C. DA Form 2769-R

D. DA Form 4669-R

5. Which regulation best describes actions a COMSEC custodian should take before INSCOM inspection?

A. AR 190-13

B. AR 380-5

C. AR 380-40

D. TB 380-41

LESSON 7

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

Item	Correct Answer and Feedback
1.	D. The CCSLA The CCSLA conducts formal audits (page 7-2, para 2a).
2.	B. A review of internal accounting and operating procedures The audit will include a review of internal accounting and operating procedures (page 7-2, par 2a).
3.	A. It is the backbone of the Army's efforts to ensure COMSEC material receives proper protection The command inspection is the backbone of the Army's efforts to ensure COMSEC material receives proper protection (page 7-3, para 3b).
4.	C. DA Form 2769-R The result of a command inspection are recorded on DA Form 2769-R (page 7-4, para 3b(3)).
5.	C. AR 380-40 AR 380-40 best describes actions a COMSEC custodian should take before INSCOM inspections (page 7-7, para 3c(3)).