COMSEC Awareness Training

Student Reading Material

June 2005

Security Solutions Group

FOR TRAINING PURPOSES ONLY

Contents

PREFACE

Omitron Security Solutions Group has developed this package to prepare personnel for the duties required in the handling and accounting of COMSEC Materials and Information.

All portions of this training will be under the direct supervision of an instructor/trainer who has been certified by a Responsible COMSEC Officer (RCO) and who has been furnished with an Instructor Guide to assist him/her in conducting this course.

Experience has shown that trainees will benefit more from this training if they study in a place free from noise and distractions and follow a planned schedule of completion.

This package is designed to acquaint the student with the general Communications Security (COMSEC) concepts.

If you have questions about the format or contents of this training package, you may contact Derek Herring at 281-853-3056 or email derek.herring@lmco.com or derek.herring@omitron.com

This page intentionally left blank

Section 1. Introduction

1.1 PURPOSE AND SCOPE

This training will be used by personnel whose duties involve the maintenance, operation or control of equipment or systems used in protection of sensitive and classified information or operations. This training will provide the trainee with information relating to Communication Security (COMSEC) and related Physical Security measures as well as their importance to protecting National Security.

1.2 COURSE OBJECTIVES

Upon completion of this training the trainee will have an understanding of:

1. Communications Security (COMSEC) Elements and Insecurities.
2. TEMPEST Considerations and Protections
3. Security Requirements

1.3 COURSE PREREQUISITES

Individuals wishing to participate in this training must:

1. Have US Citizenship
2. Be a Permanent Government or Government Contractor Employee
3. Have a position in which their duties require them to have access to or knowledge of classified or sensitive information.

Section 2. COMSEC Overview

You may already be aware of your agency's or contract's security programs by now, and are asking yourself, "Why do I need more information on security?" The answer to this question is simple. Despite all the security training, security warning posters, and other reminders, classified and sensitive information is still being disclosed to unauthorized personnel. Foreign intelligence-gathering activities continue despite our precautions. Therefore, we must continue to regularly educate all personnel about security, especially in the areas of communication security (COMSEC). The success of our security program requires effort from us all.

Our coverage of communications security (COMSEC) in this course is mainly concerned with the means of communication in which transmitting and receiving information require wire or radiant energy. It should be clear that our National Security is dependent on the security on the systems providing these electronic transfers. Ideally, only the intended or authorized parties receive these transmissions in a usable format, and any unintended or unauthorized receipt of the transmissions is unusable by the recipient. In the following paragraphs we discuss the COMSEC elements used in that protection and the COMSEC security incidents that could jeopardize such protection.

2.1 ELEMENTS OF COMSEC

COMSEC is the protection afforded classified and sensitive information or operations that is achieved by applying the following four elements:

1. Transmission Security (TRANSEC) – The protection of information when it is passed between parties.

2. Cryptographic Security – The proper design, implementation, use and protection of Cryptographic (Encryption/Decryption) systems used for the protection of information.

3. Physical Security – The means by which unauthorized parties are denied access to information and materials.

4. Emissions Security – The means by which unintentional emanations are limited or stopped from leaving the security of a controlled space.

These four elements of COMSEC are used to deny unauthorized persons/parties information of value, to support operational access to systems, and/or to ensure the authenticity of such telecommunications. Why do we need COMSEC? The answer is simple. COMSEC prevents unauthorized persons from obtaining information of intelligence value and/or gaining access to (would "knowledge of" be better?) sensitive operations resulting from the interception and analysis of our communications.

Section 3. Transmission Security (TRANSEC)

TRANSEC is that part of communications security that includes all measures (except physical protection) designed to protect transmissions from interception and exploitation by means other than crypto analysis. Everyone must use transmission security, because everyone uses at least the telephone in the performance of their duties. Examples of transmission security include:

1. Changing radio frequencies and call signs.
2. Using message format for classified record communications.
3. Using classification guides to determine whether or not certain information should be sent over unsecure systems.
4. Using cryptographically secured telephones, voice circuits, and air/ground communications systems.
5. Canceling or altering communications patterns to prevent detection of a change from normal traffic flow and volume.
6. Using authentication to ensure validity of receipt of traffic and to counter telecommunications systems intruders.
7. Using authorized codes when unsecure telephone or radiotelephone communications are used.
8. Imposing radio or telephone silence.

3.1 MODES OF TRANSMISSION

For official information to be useful, it is normally passed from one person to another. The various means of passing information are called modes of transmission. These modes of transmission may be electromagnetic or nonelectromagnetic.

3.1.1 ELECTROMAGNETIC TRANSMISSION

Signs, signals, writing, images, and sounds or information of any type when sent or received by wire, radio, light, or other electromagnetic systems are electromagnetic telecommunications. Modes of electromagnetic transmissions are radio, telephone, television, radar, data-link, teletype, and facsimile.

3.1.1.1 Radio

When we talk about radio communications, we normally think of air-to-air, air-to-ground or ground-to-ground. Examples of radio communications include pilots talking to each other or to the control tower and security police talking on their hand-held radios. These forms make up only a small percentage of the total radio communications. Virtually all electromagnetic telecommunication systems

transmit by radio signals. For example, microwave radio signals can travel well beyond the equipment--as easily as you tune in your favorite radio station at home. Radio is one of the fastest modes of communication because it is available to virtually everyone within an instant. However, because it is impossible to control the number of listeners, radio is also the least secure. Classified information or information of possible intelligence value must never be sent by radio unless approved secure crypto-equipment or codes are used.

3.1.1.2 Telephones

The telephone is one of the fastest, most convenient, and most widely used communication modes in use today. All government sites and installations, as well as contractor facilities, are connected to telephone networks. In addition, government (FTS), military (DSN) and commercial long-distance telephone networks provide connections to virtually any telephone number, governmental, military or civilian, within the United States and overseas. These systems have one drawback—they are not secure. While the telephone is one of the fastest and most convenient modes of transmission, it offers no security. Classified, sensitive, and information of possible intelligence value must not be discussed over these unprotected systems. Approved secure encryption systems must be used for such communications. In summary, never discuss classified or sensitive information on any unsecure electromagnetic transmission device.

3.1.1.3 Cellular Telephones

The use of cellular telephones has been on the rise over the last ten years, and today they are getting more use than the normal telephone. We use our cell phones at home, in the car, at the mall, at work, virtually everywhere; making cell phones a very high risk to security. Also, because cell phones are more like handheld radios, their transmissions are easier to monitor or intercept. In short, the use of cellular telephones can be very convenient but this convenience can have a devastating effect on security if they are not used in a safe and security minded manner.

3.1.1.4 Email

Next to the use of telephones and cellular telephones, email has become one of the most convenient and widely used forms of communication in the world today. Again almost all government sites and installations have email domains along with most contractors. As email becomes more and more popular, its risk to security also rises. Unless an approved form of encryption is applied, email should not be used to transmit sensitive information and email can never be used to transmit classified information.

3.1.2 NON-ELECTROMAGNETIC TRANSMISSION

Non-electromagnetic communications include any form of transmitting or receiving information without the use of an electromagnetic medium. Non-electromagnetic

transmissions include talking face-to-face and hand delivery of information such as performed by couriers and the postal service.

3.1.2.1 Face-to-face

This method of communication occurs whenever two or more persons are in the same area and have a conversation. In most cases this is a very secure means of communications.

3.1.2.2 Hand Delivery

This method of communication is when information in a hardcopy form is carried to its recipient. This transferal of information can be performed person-to-person or by means of courier or some form of postal service. Again in most cases this is a very secure means of communication, but it can vary depending on the means used for the transferal.

Section 4. Cryptographic Security

Cryptographic Security or Cryptosecurity includes designing and using technically sound crypto systems. Cryptographic systems are used to protect classified and sensitive data transfers between all Government and Military Agencies. These systems range from highly classified Type 1 Military rated systems to sensitive but unclassified (SBU) commercial off the shelf (COTS) systems.

No matter the classification, or rating for the crypto system, the basic measures for protecting the system from comprise are the same. These basic measures are:

1. Strictly follow operating instructions and procedures.
2. Never transmit in both clear and encrypted modes at the same time, nor should the same information be transmitted in both the clear and encrypted modes over the same lines.
3. Always perform key changes within specified times.
4. Never use key material not designed or intended for a specified system.
5. Never discuss specific crypto system processes, configurations, keying material or operational procedures outside of a cryptographically secure area or over an unsecure telephone.
6. Never allow uncertified personnel to perform operations or maintenance on a crypto system.

Although all of the above are key elements used in the protection of crypto systems, the most effective measure of protecting these systems is to limit all information in these systems to as few personnel as possible. The fewer persons who have the information, the less likely the information will be disclosed to unintended persons.

Section 5. Physical Security

Physical security is the part of COMSEC that results from taking all physical measures necessary to safeguard classified material from access or observation by unauthorized persons. All personnel who come into contact with classified or sensitive material must use physical security measures. Physical Security entails many elements that aid us in keeping control over the classified and sensitive materials in our safekeeping. These elements include but are not limited to guards, safes, alarm systems and methods of identification. Without good physical security, the other efforts of our overall security system would be in vain.

5.1 STORAGE OF CLASSIFIED OR SENSITIVE MATERIALS

The General Services Administration (GSA) establishes and publishes uniform standards, specifications, and supply schedules for containers, vault doors, alarm systems, and associated security devices suitable for the storage and protection of classified and sensitive information and material throughout the government.

When classified or sensitive material is not under the personal control and observation of an authorized person, it must be guarded or stored in a locked security container. Because most personnel will not be dealing with Top Secret information, its storage requirements will not be covered.

5.1.1 Secret and Confidential

The minimum requirement for information and materials that have been classified as Secret and/or Confidential is storage in a GSA approved Security Container having a built-in, three position, dial-type combination lock. However, it is recommended that, when available, this information be stored in a Class “B” Vault.

5.1.2 Sensitive but Unclassified (SBU) COMSEC

The minimum requirement for SBU COMSEC information and materials is storage in a steel filing cabinet equipped with a steel locking bar, provided it is secured by a GSA approved changeable combination padlock. However, even though it is not required, where feasible, SBU COMSEC can and should be stored using the same type of containers or vaults as Secret and Confidential materials.

5.1.3 For Official Use Only (FOUO)

At a minimum, FOUO materials should be stored in a limited access area or in a lockable container. However, even though it is not required, where feasible, FOUO can and should be stored using the same type of containers or vaults as Secret and Confidential materials.

5.2 HANDLING AND USING MATERIALS

Custodians of classified and sensitive material are responsible for protecting and accounting for such materials 24 hours a day, 365 days a year. Custodians are responsible for locking classified and sensitive material in proper security containers when it is not in use or under the direct supervision of authorized persons. Custodians must follow procedures that ensure not only that unauthorized persons do not gain access to classified and sensitive information or material by sight or sound but also ensure that classified and sensitive information is not discussed with or in presence of unauthorized persons.

5.2.1 During Working Hours

Each individual must take precautions to prevent access to classified and sensitive information by unauthorized persons. Always be aware of your surroundings, think before you speak over unsecure communication lines, and ensure materials entrusted to you receive continuous protection.

5.2.2 Removal from Storage

When classified and sensitive documents are removed from storage for working purposes, they must be kept under constant surveillance and placed face down or covered when not in use.

5.2.3 End of Duty Day

All heads of activities must require (does “establish” sound better?) a system of security checks at the close of each working day to ensure that the classified and sensitive material held by the activity is properly protected. Managers of classified and sensitive material are responsible for conducting an inspection that ensures:

1. All classified and sensitive material is accounted for, and stored in the manner prescribed.
2. Burn bags are properly stored or destroyed.
3. The contents of wastebaskets that contain classified and sensitive material have been properly stored or destroyed.
4. Classified and sensitive shorthand notes, carbon paper, carbon and plastic typewriter ribbons, rough drafts, and similar papers have been properly stored or destroyed.

5.2.4 Taking Work Home

You may not remove classified and sensitive information or material from officially designated office or working areas to work on it during off-duty hours or for other purposes involving personal convenience. No matter how urgent the need to complete a project, removing classified and sensitive materials from secure areas

is never a good idea and may constitute a security violation. It is an exceptionally bad idea to even consider taking these items home. This includes discussing any classified or sensitive information with loved ones. In most cases, your spouse and your children will not understand that the information you have provided could have national security ramifications and will quickly pass the information on to friends and other family members.

5.3 CONTROL ACCESS AREA (CAA)

As the name implies, a CAA is an area into which entrance is controlled. Only authorized personnel are allowed entry, and even they must first be properly identified or recognized by the person or system controlling the entrance. Only those persons having a proper security clearance or background check, a need to know, and proper identification are authorized to enter.

5.3.1 Access Authorization

Only after personnel are granted a clearance or their background checks have been completed are they determined eligible for access to classified or sensitive equipment, information or areas. This does not mean they have unrestricted access to all classified or sensitive equipment, information or areas. Their level of “need to know” must be assessed, and they may only be granted access, in writing, by the Designated Authorizing Officer (DAO) to the controlled equipment, information and areas within their level of need to know required to perform their assigned duties.

5.3.2 Escorted Access

At times, personnel who do not have access to an area will need to enter the controlled area. Normally, the DAO will authorize their entry. Under emergency or unusual operational conditions, the shift Leads or other designated personal may also be authorized to admit “escorted only” visitors. Upon entering the area, these personnel must be signed-in on the Visitor Register. This form provides a record of the visitor’s arrival and departure times, as well as the name of the person authorizing the visitor's entrance. Usually, the person authorizing entrance will act as the escort for the visitor. Other personnel working within the area may have this escort duty delegated to them.

5.4 METHODS OF IDENTIFICATION

For any access control system to be effective, there must be a method to identify personnel authorized to access an area. There are many methods that can be used for identifying personnel, including biomedical scanners seen in 007 movies, but for most government and contractor facilities there are only three currently in use. These methods are discussed in the following paragraphs.

5.4.1 Personal Recognition

The best security control system operating today is that of personal recognition. In small locations, where it is easy to recognize each individual authorized access, strangers appearing in the facility can be easily spotted. Anytime you see an unescorted individual whom you do not recognize in the secure area, it is your duty to check his or her authority for being in that area, and take appropriate action to remove the individual from the area if necessary. This method however has limitations, which would make it necessary for persons controlling the access to an area to personally know all individuals having access.

5.4.2 Access Lists

This method of access control is used by placing the names of authorized personnel on an official entrance list. This list is limited to the names of persons who have regularly assigned duties within the secure or controlled area and others whose duties require them to have frequent access. Even with this list, a person in control of the area's access must be able to identify the individual prior to granting entry.

5.4.3 Security Badges

This is the most widely used method of access identification used today. The security badges that are used normally have each individual's picture on the front and some type of authorization or approval on the back. Badges can have a magnetic strip or some type of passive electronics that are used by readers at entry points to ascertain if the individual is authorized to enter an area. Although security badges are the most widely used method, they should never be the sole means of access to classified or sensitive areas.

Section 6. Emissions Security

The purpose of emission security is to deny unauthorized persons information of value, which they might derive by intercepting and analyzing compromising (unintentional) emissions from cryptographic equipment and/or telecommunications systems. Those who install, use, or maintain cryptographic and telecommunications equipment and computer input-output devices should be aware of emission security requirements.

6.1 TEMPEST

TEMPEST is an unclassified short name referring to the investigation and study of compromising emanations, usually electromagnetic or acoustic in nature. TEMPEST is often used synonymously with “compromising emanations.” Any electrical information-processing equipment may generate compromising emanations if the equipment is processing classified or sensitive information. Compromising emanations travel through space, over telephone lines, water pipes, and other conductors leaving an area.

6.2 TEMPEST COUNTERMEASURES

Because of the wide-ranging nature of the threat, rigid and categorical application of all approved countermeasures is neither practical nor necessary for a facility to be in compliance with the policy on the control of compromising emanations (CE). The vulnerability or exploitation risk determined by an analysis of the system that is performed using applicable TEMPEST documents for the given situation will dictate the countermeasures necessary for the protection of the information being processed. Generally, selecting equipment that meets TEMPEST standards and follows basic RED/BLACK installation standards in combination with appropriate physical security provides adequate protection. However it is not always possible or practical to use equipment that meets TEMPEST standards. Therefore, there are several countermeasures that can be applied to minimize TEMPEST problems.

For more information on TEMPEST and TEMPEST Countermeasures you can contact your COMSEC Account Manager or Responsible COMSEC Officer.

Section 7. Information and Classifications

In most cases when personnel hear the term COMSEC they think of highly classified information, materials and equipment. However this is not always the case when dealing with COMSEC. In fact, the compromise of information that is considered sensitive and is, in most cases unmarked, poses just as much a threat to the overall security. The following paragraphs will explain the different types and classifications of information that are in use by government and contractor personnel.

7.1 MARKED INFORMATION AND MATERIALS

Information and materials that are marked based on their importance are very easily identified. They receive their markings or classifications based on the amount of damage that would be done to National Security or the mission of the classifying agency. The following are types and definitions of marked information or materials with which you may come in contact.

7.1.1 TOP SECRET

This designation shall be applied to information or material, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security.

7.1.2 SECRET

This designation shall be applied to information or material, the unauthorized disclosure of which could reasonably be expected to cause serious damage to national security.

7.1.3 CONFIDENTIAL

This designation shall be applied to information or material, the unauthorized disclosure of which could reasonably be expected to cause damage to national security.

7.1.4 FOR OFFICIAL USE ONLY (FOUO)

This designation shall be applied to information or material, the unauthorized disclosure of which, could pose a threat to the operations, or mission of the government or classifying agency.

7.1.5 SENSITIVE BUT UNCLASSIFIED (SBU) COMSEC

This designation shall be applied to information, equipment or materials the unauthorized disclosure of which could pose a threat to the operations or mission being protected.

7.2 UNMARKED INFORMATION AND MATERIALS

On a day-to-day basis everyone who works in and around government facilities uses information and/or materials that are highly sensitive. However, in most cases we are unaware that the information or materials we are using are sensitive, and their unauthorized disclosure could very likely place some element of national security at risk.

Why are we unaware that the information and materials we are using are sensitive? The answer is, these materials and information are in most cases unmarked, having no identification as to their sensitivity. Below is a list of information and materials that should always be considered to be sensitive:

1. Passwords
2. Lock Combinations
3. IP Addresses
4. Phone Numbers of Dial-in Modems
5. System Diagrams/Configurations
6. System Vulnerabilities
7. Operational Contingency Plans
8. Security Control Measures
9. Security Incident Reports
10. Personal and Privacy Act Data

Section 8. Disclosing Information

As a person who possesses classified and sensitive information, you must know when disclosure is authorized and how to prevent disclosure when it is not authorized.

8.1 Authorized Disclosure

Do you know what is meant by the term “authorized disclosure”? Quite simply, it is giving classified or sensitive information to an authorized person. You should ensure that any recipient of classified or sensitive material/information in your control meets the following three requirements for possessing classified and sensitive material.

1. Has official duties requiring (“which provide”?) a need to know
2. Possesses a proper clearance or background check
3. Possesses proper identification.

8.2 Unauthorized Disclosure

Now that you know the meaning of “authorized disclosure,” we need to discuss its opposite, “unauthorized disclosure”. An unauthorized disclosure means that classified or sensitive information/materials have been provided to an individual who does not meet all three of the requirements of an authorized disclosure. For instance, assume that Joe Smith has a secret security clearance and proper identification. He works at the same facility as you, but in a different organization or on a different contract. If you give him classified or sensitive information about your area, your duties or types of equipment or information you handle, and he did not have a need to know, you would be committing a security violation of unauthorized disclosure.

8.3 UNINTENTIONAL DISCLOSURES

Most unauthorized disclosures of classified and sensitive information are made unintentionally for reasons of shortness of time, lack of planning, or a lack of knowledge of the threat. The following paragraphs will identify these reasons of unintentional disclosures and how to prevent getting caught in one of these scenarios.

8.3.1 Unaware of Surroundings

There are two basic scenarios where unintentional disclosures are caused by personnel not being aware of their surrounding:

1. The first scenario is a situation where a telephone is not protected from background conversations while in use. For example, you lay the telephone handset on a desk or console while looking for something and you do not inform other people in the room that the telephone is being used. One factor we must keep in mind is that the telephone mouthpiece is a sensitive microphone that can pick up and amplify noises and conversation in the background. The correct procedure is to inform those in the room that there is an “open phone” so they do not discuss classified or sensitive information in the area until you have finished transacting your business.

2. The second scenario is a situation where you are having a classified or sensitive discussion with another authorized individual in an uncontrolled area. These uncontrolled areas could be conference rooms, hallways and even elevators. This is fine in most cases as long as no one else is in the area, but if you are not paying close attention to your surroundings and continue your discussion after an unauthorized individual enters the area, an unauthorized disclosure of information is likely to occur.

8.3.2 Trapped by Time

Another situation in which classified and sensitive information may accidentally be given over the telephone occurs when you are trapped by time. This situation is usually a result of poor planning or events out of norm. It is sometimes a case in which you feel there is just not ample time to deliver the information in person and that you had to use the telephone to meet a deadline or pass along information to a superior.

8.3.3 Awe of Position

Awe of position can cause classified and sensitive information to be given over the telephone. Just because the person wanting the information holds a high position is no reason to give classified or sensitive information over the phone. If you get caught in this situation, inform the caller that the information is classified or sensitive, and you will deliver the necessary information properly.

8.3.4 Emotional Hazard

It is possible that one can get so emotionally involved in a telephone conversation that classified and sensitive information is given out. This situation is known as emotional hazard. For example, you receive a phone call asking when you will complete the Communication Interface Checkouts. Angrily you reply, “I can't even start until the New Mission Keys have been loaded in the KGs”. Since you were a little unhappy because others were affecting the performance of your duties, you inadvertently divulged classified or sensitive information over the telephone.

8.3.5 Failure to Think

Nearly all unintentional disclosures of classified and sensitive information can be summed up in three words, “Failure to Think.” You are engaged in unclassified gossip when you use DVIS to “shoot the breeze” with your friend or make small talk while waiting for Sim Configuration to be completed. Sometimes a comment divulges more classified or sensitive information that you realize. For example, a friend calls you and asks you to go fishing over the weekend. You answer that you cannot get the time off since you have to setup so many keys before 0500 hours on Monday. At first this does not seem like much of a disclosure. However, by knowing the area in which you work and other bits of information, an unauthorized person could determine there is a mission to be launched at 0500 hours on Monday and there will be a new set of crypto keys in use.

8.4 ATTEMPTS TO DISGUISE INFORMATION

Persons who deliberately try to conceal or disguise the meaning of what they are saying further increase the security threat posed by the ordinary telephone. Although these attempts are less numerous than accidental disclosures, the results are far worse. The following paragraphs identify the methods personnel use in attempts to conceal or disguise information.

8.4.1 Talk-Around

Earlier we mentioned that to speed things up, you may try to disguise classified and sensitive information and use the telephone anyway. “Talking around” is a technique in which you try to get the information across to the recipient in a manner you believe will protect it. However, no matter how much you try to change words about a classified or sensitive subject, it is still classified or sensitive. If you refer to parts of a classified or sensitive system as “the thing in the lower right of the big black box under the monitor” you have attempted to “talk around” and disguise classified or sensitive information. However, any person who would go to the trouble of monitoring a telephone conversation would know enough to determine what you actually meant.

8.4.2 Self-Made References

Another common way of trying to get by with discussing classified and sensitive information on the phone is the use of a self-made reference system. This is an attempt to encipher your conversation by using your own system. This system rarely works because few people are clever enough to refer to an item of information without actually revealing names, subjects, or other pertinent information that would reveal the classified or sensitive meaning.

8.4.3 Paraphrasing

Paraphrasing is very closely related to talk-around. The main difference is that talk-around gives the appearance of double talk. Paraphrasing is using different

words to say the same thing. Again, anyone who would take the trouble to monitor the phone could see through paraphrasing.

8.4.4 Incomplete Reference

Another way of getting around security classification is using incomplete or partial references. If you were talking about the KG-84 on the phone and referred to it as the 84, it would be ridiculous to assume that an eavesdropper would not know what 84 really means and its stated specifications.

Section 9. Security Incident

Security Incidents are events or incidents that jeopardize any of the COMSEC Elements. Security Incidents can be broken into three categories that are; Personnel, Physical and Cryptographic.

9.1 Personnel Security Incidents

These types of security incidents are basically categorized as those that involve a person or persons in the act of committing espionage or sabotage of COMSEC Equipment, Keys, Systems or other materials, or trying to hinder the use of the systems information so that it adversely affects the mission.

Personnel Security Incidents also include the capture, defection, recruitment (either real or attempted) by hostile agents, or unauthorized absence of individuals having knowledge of COMSEC Equipment, Systems, Keys or operational principles.

9.1.1 Examples of Personnel Security Incidents

1. An unauthorized person found monitoring and/or recording data or voice transmissions.
2. An unauthorized person found cutting or altering data or voice transmission cables.
3. A Cryptographic maintenance person who does not return from a scheduled vacation and his whereabouts and contact information is unknown.
4. A person approaches a Cryptographic maintenance or operations person and attempts to garner information on his duties and responsibilities.

9.2 Physical Security Incidents

These types of security incidents are categorized as the loss of physical control over COMSEC Equipment, Systems, Keys or other materials. These insecurities can range from forgetful acts by authorized persons to acts of espionage by hostile agents.

9.2.1 Examples of Physical Insecurities:

1. COMSEC Key Material cannot be accounted for, and is believed lost.
2. Evidence of tampering with locks or seals that protect COMSEC Equipment or Systems.
3. Coping of any Key Material.

4. Receipts of any COMSEC Equipment or Materials that are either not packaged correctly or show evidence of tampering with the package.
5. Unauthorized person(s) gains access to COMSEC Equipment or Materials.
6. Discussion of COMSEC information or insecurities in the presence of unauthorized persons or over unsecure communication systems.

9.3 Cryptographic Insecurities

These insecurities are generally any actions or inactions that place a Cryptosystem or its associated Keying material in jeopardy of compromise.

9.3.1 Examples of Cryptographic Insecurities:

1. Any unauthorized modifications or component replacement on COMSEC Equipment.
2. The unauthorized extension of a cryptoperiod.
3. Simultaneous transmission of the same data in both plaintext and ciphertext modes.
4. Transmission of the same data in both plaintext and ciphertext over the same lines.
5. Use of maintenance, test or exercise keys for other than their intended purposes.

9.4 REPORTING INSECURITIES

It is paramount that any known or suspected security incident or compromise of classified or sensitive COMSEC material be reported immediately. Each government or contactor location or facility must have a documented reporting process. This process must detail who shall be notified in the event of any suspected insecurity.

It must also be noted that when reporting any suspected security incidents most of the initial notifications will be performed over unsecured telephones or other communications. This means that no details of the suspected incident can be discussed during this notification. If details of any suspected incident are discussed over an unsecured means of communication, then a second security incident has been committed. When these notifications are made, very generic statements should be used, for example; “We have an issue and need you to report to work”. If all personnel involved in the reporting process understand the use of this type of generic statement then no further details are necessary over unsecured communications.