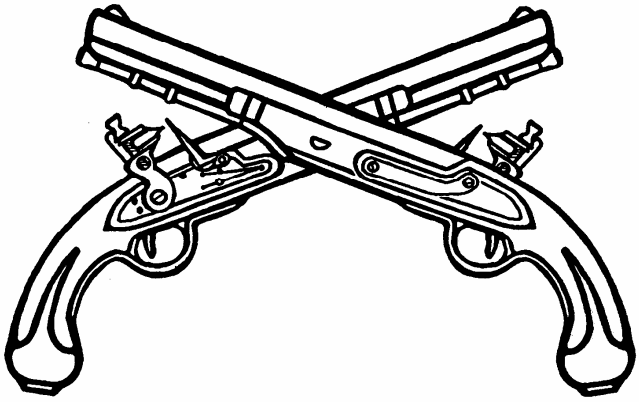
SUBCOURSE
MP1002

EDITION
C

AREA SECURITY

MP



SETS THE STANDARD FOR EXCELLENCE

THE ARMY INSTITUTE FOR PROFESSIONAL DEVELOPMENT

ARMY CORRESPONDENCE COURSE PROGRAM

AIPD

READINESS / PROFESSIONALISM

THRU GROWTH

AREA SECURITY

Subcourse Number MP1002

EDITION C

United States Army Military Police School
Fort Leonard Wood, MO 65473-8929

5 Credit Hours

Edition Date: January 1996

SUBCOURSE OVERVIEW

We designed this subcourse to teach you to identify the need for security and to implement appropriate security measures to counter the threat.

There are no prerequisites for this subcourse.

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 otherwise stated, the masculine gender of singular pronouns is used to refer to both men and women.

TERMINAL LEARNING OBJECTIVE

ACTION: You will identify the need for security and the security measures to implement.

CONDITION: You will have this subcourse, paper and pencil.

STANDARD: To demonstrate competency of this task you must achieve a score of 70 percent on the final subcourse examination.

TABLE OF CONTENTS

LESSON 1

OPERATIONS SECURITY (OPSEC)

Critical Task: 191-386-0009

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn to define OPSEC, determine OPSEC in the hostile intelligence threat, and determine OPSEC guidelines and training.

TERMINAL LEARNING OBJECTIVE:

ACTION: Define OPSEC, its guidelines, and training requirements.

CONDITION: You will have this subcourse, paper and pencil.

STANDARD: To demonstrate competency of this task you must achieve a score of 70 percent on the final subcourse examination.

REFERENCES: The material contained in this lesson was derived from the following publications: AR 530-1 and FM 19-30.

INTRODUCTION

Operation security helps to avoid disclosure of sensitive information. Such data concerns a unit's mission, capabilities, research and development. It also includes training which could prevent the compromise of military operations.

1. Definition of Operations Security (OPSEC).

a. OPSEC (which is covered by AR 530-1, Fig. 1-1) is the protection of military operations and activities. Such protection results from the identification and final elimination or control of intelligence indicators. We refer to these indicators as vulnerabilities. These are those areas susceptible to hostile attack. Military operations and activities include peacetime and combat operations. Also included are exercises and contingency planning.

b. OPSEC is designed to protect operations and activities from being compromised by any hostile intelligence service. A basic OPSEC program consists of the following main areas:

(1) Physical Security.

(2) Information Security.

(3) Signal Security.

(4) Deception.

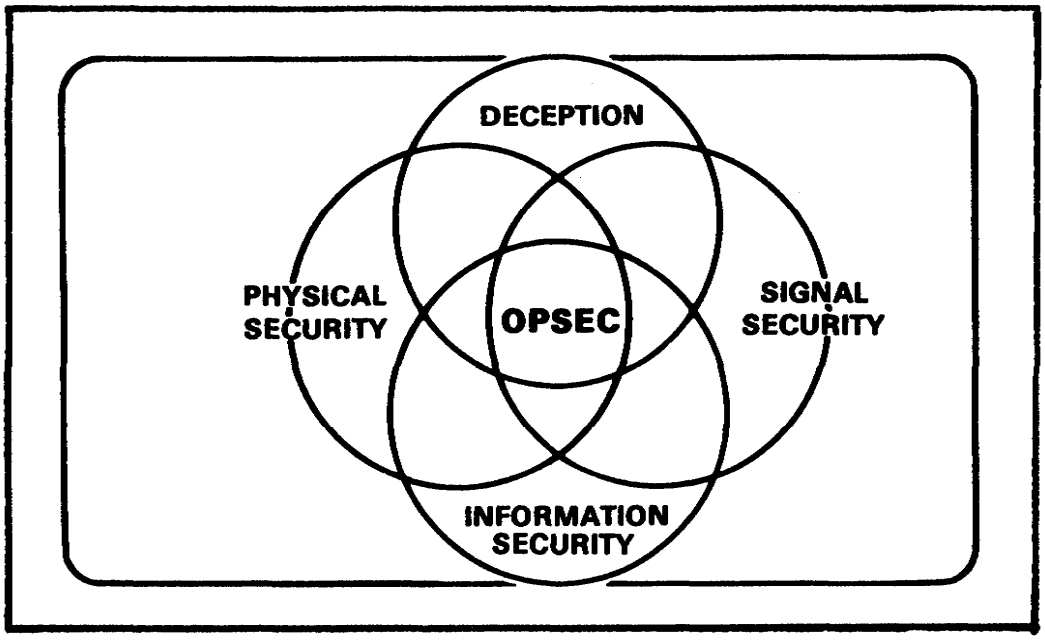


FIGURE 1-1. OPSEC

c. An active OPSEC program continually rates each operation. Evaluation is based upon all known intelligence collection methods. This program also assesses vulnerabilities. Then measures are begun to reduce or negate collection efforts against those areas.

d. OPSEC is the concern of COs, staffs and persons at all levels of command. Units and individuals set up steps necessary for good OPSEC. In order to do this, these people must train; they must be able to use proper techniques and procedures. OPSEC is a part of all operations. An ineffective program results when people do not believe OPSEC is important.

e. The result of a good OPSEC program is force security. Again, this requires an integrated effort by everyone concerned. OPSEC is adapted to fit the operating traits, techniques and needs of each organization. Each unit takes those steps necessary; these steps should provide security and retain the element of surprise. The goal of each unit is to keep the enemy from learning what the friendly unit is going to do. The intelligence threat to US military operations today is great, and it continues to grow. Potential enemies are daily working to gain information. They seek data regarding our capabilities and limitations; they want to know our intentions and plans; they want data on our tactics and readiness. The enemy finds certain data valuable and exploitable. Examples are our communications patterns and stereotyped

procedures. Also, many types of unclassified information are of value to them. Many of these sources are often overlooked as potential security breaches. OPSEC considerations must be fully integrated into all daily duties. This should be done in addition to integration into special highly sensitive operations. OPSEC is a command responsibility.

2. OPSEC and the Hostile Intelligence Threat.

a. The most serious threats to the security of Army operations and activities are hostile intelligence services and their agents. Continuous emphasis by these services is placed on collecting data. Such data, of course, relates to the U.S. and allied forces military capabilities. It also concerns research, development, and industrial techniques.

b. There are means of protecting classified and/or sensitive information from unauthorized disclosure: the Army's OPSEC activities are used to counter these threats. Those means are as follows:

(1) Human Intelligence (HUMINT).

(2) Signal Intelligence (SIGINT).

(3) Imagery Threat Photographic Intelligence (PHOTINT)/(IMINT).

(4) Electronic Warfare (EW).

3. Human Intelligence (HUMINT).

a. HUMINT is the intelligence obtained by using people to gather items of data. HUMINT collection involves both overt and covert operations. Examples of overt operations would include data obtained from public records and publications; covert operations include inducing people to disclose information. It also includes eavesdropping on conversations and/or conducting surveillance operations. HUMINT may include sources as diverse as friendly troops who report information about the enemy. These troops report on interrogations of prisoners, defectors, and refugees; also, they report on counterintelligence sources. Troops will include statements made by officials of foreign countries and they will report on terrorist activities. However, the individual soldier is usually the most important HUMINT source.

b. The enemy has many ways of collecting data, and any number of these methods could be targeted any time and in varying degrees of intensity. We do have procedures which can deny or hamper the enemy's collection threat. This is true regardless of the enemy's methods. The procedures are not necessarily new; the US Army has used many of them before. All procedures which keep the enemy from collecting data, giving him a tactical advantage, are grouped under OPSEC.

4. Signal Intelligence (SIGINT). SIGINT is intelligence that is obtained by intercepting electronic signals. This data is gathered by intercepting

telecommunications signals; it may also be obtained by intercepting electromagnetic radiations.

a. Interception of electronic signals. Examples are the interception of telephone or radio conversations. Such action is handled by Communications Intelligence (COMINT).

b. Interception of electromagnetic signals. Such signals are non-data related radiations. Radar signals are an example. Action relating to such interception is called Electronic Intelligence (ELINT).

5. Signal Security (SIGSEC). This is an overall term referring to communications security measures. Such measures are taken to deny enemy collection of data from COMINT and ELINT operations. By listening to our electronic emissions, the enemy gains information. This data relates to our dispositions, operations, etc. Such data can be fed directly into the collection system for their intelligence use. Also, they gain data about our electronic systems. They then use it in planning actions to reduce our combat effectiveness. They can accomplish their plans by interfering with those systems.

6. Compromising Emanations. Data may also be obtained by the enemy through compromising emanations. These are unintentional and may be data related or intelligence-bearing impulses. These impulses may be electrical, magnetic, or acoustical. They are emitted by or come from any electrically run, data-processing equipment or facility. Such impulses relate to the preparation, transmission, receipt, storage or retrieval of classified data. Examples are electric typewriters and crypto equipment. Automatic data processing equipment is another example. Control of these emanations (TEMPEST) is a further counter to the SIGINT threat.

7. Imagery Threat. Some intelligence is derived mainly from radar, infrared, and photographic sensors carried by overhead platforms. To assure timeliness, intelligence gained from imagery must be disseminated to COs electronically. This is done as opposed to sending them photographically. Imagery can be the most accurate data for the production of intelligence, but it is limited. Weather, hostile countermeasures, and often, lack of timeliness are limitations. Within the intelligence community and throughout the military, imagery may also be referred to as PHOTINT. This is an acronym for photographic intelligence.

8. Electronic Warfare (EW). The EW threat consists of electronic warfare support measures (ESM), and electronic counter measures (ECM). Actions are taken by ESM to search for, intercept, identify or locate sources of radiated electromagnetic energy. All of these must have immediate threat recognition. Jamming and electronic deception involves ECM. Such actions are necessary to prevent or reduce the use of the electromagnetic spectrum.

9. Military Deception. Activities are designed to mislead the enemy regarding friendly intentions. This is done by employing visual, sonic, electronic, olfactory, or other means. The goal is to manipulate, distort,

Falsify, or deny evidence of intended or current operations or activities. By so doing, the enemy is induced to react in a way prejudicial to his best interest.

10. OPSEC Analysis Procedures. The OPSEC analysis procedures are accomplished through four steps. The first two are analysis and selecting the correct protective measure; the second two are choosing countermeasures and surveys. These steps correspond respectively to the planning, execution, and after-action of an operation.

a. Analysis. Conducting an OPSEC analysis is part of the normal staff work. Analysis must be done in planning each phase of an operation. Three things have to occur:

(1) Estimating the Hostile Intelligence Threat. Once the S3 has stated the mission, estimation is done by the S2. The S2 coordinates with the communications-electronic offices, supporting Army Security Agency (ASA) elements, and other sources. Their aim is to find answers to two very important questions: "What are the enemy's intelligence collection capabilities?" "What are the intelligence collection resources of the enemy CO directly opposing us?" The S2 will try to determine the impact of those enemy capabilities used in the immediate area.

(2) Determining the Sensitive Aspects of the Operation. This task is a joint effort of S3 and S2. They must answer the question: "If known by the enemy, what information, in what time frame, could compromise the operation?" Some essential elements of friendly information (EEFI) are:

(a) The objective.

(b) The unit conducting the attack.

(c) Task organization.

(d) The reserve location and its composition.

(e) The command post.

(f) The morale of the unit.

(g) The unit strength.

(h) Logistical problems.

(i) The combat service support activity, location and movement.

(3) Determining OPSEC Vulnerabilities. This effort is a function of the S3. He coordinates and reviews staff actions necessary to accomplish the mission. He must answer the question: "If known by the enemy, what staff actions, in what time frame, could provide EEFI?"

b. Selecting the Developing Protective Measures. OPSEC measures are implemented to degrade hostile intelligence agencies' collection capabilities.

c. Countermeasures. Once a threat against a unit, installation, or activity is identified, an assessment is made. It will concern the vulnerability of each individual EEFI. First, the assessment determines how vulnerable an EEFI element is to collection efforts; second, an appropriate countermeasure can then be chosen and implemented. A countermeasure is an action taken to eliminate or reduce the vulnerability of and EEFI element to collection. Examples are physical security precautions, security awareness when using telephone or radio communicators, camouflage techniques, etc. Such countermeasures are used to deny a hostile intelligence service the chance to collect any data that would compromise the operation, activity, or project.

(1) The principal elements of OPSEC are physical security and information security; other principals are signal security and, at times, deception operations. Physical security measures are perimeter fencing, badge and pass system, protective sensors, etc. These measures can greatly aid in implementing an OPSEC program. Further information concerning physical security measures can be directed to the local provost marshal office. Information security is the protection of information and documents. This is vitally important to the OPSEC program.

(2) Security procedures may include using only approved storage containers, double-checking of offices before leaving, etc. Such measures can be taken by persons to protect classified and sensitive information from compromise. AR 380-5 covers DA Information Security Program Regulation. It contains important provisions regarding information security and can be used to aid in implementing the OPSEC program.

(3) Signal Security (SIGSEC) includes all measures taken to deny collection of data from both COMINT and ELINT operations. However, such a simple thing as not discussing classified or sensitive information over the telephone can greatly aid in maintaining security. Deception operations are security measures taken to deceive, mask, or mislead any collection effort. Camouflage systems for vehicles, equipment, and personnel are simple deception measures. The use of detailed deception operations is tightly controlled, and procedures outlined in applicable regulations and guidelines should be consulted. This should occur before beginning a deception operation.

d. OPSEC Surveys.

(1) An OPSEC survey is an investigation of the intelligence indicators projected by an operation or activity. The goal is to determine what an enemy can know and what his potential sources are. The survey is an intelligence collection effort. Minimal overt manpower is used. The survey is conducted in a limited time frame. It is important that members of the surveyed unit and COs at every level understand that the survey is a fact-finding service; it is not a fault-finding service.

(2) If the OPSEC of an activity or agency is to be enhanced, a first step should be an OPSEC survey. Detailed instructions in planning and conducting surveys are found in the JCS booklet, OPSEC Survey Planning Guide (U). An initial survey may indicate the need for further diagnostic assistance. If so, then specialized counterintelligence services should be considered. These services include procedure and policy survey and penetration operations at sensitive areas. Services also include technical surveys, computer surveys or the more complete OPSEC surveys.

11. OPSEC Training.

a. OPSEC training is conducted to enable all personnel (1) to recognize OPSEC degrading procedures, and (2) to understand guidance which has been included in directives to enhance OPSEC. Also, operations and activity planners receive special training. This enables them to avoid the inclusion of OPSEC degrading factors in the directives governing their operations. Such training also enables them to include as many OPSEC enhancing measures as possible.

b. Indoctrination briefings are intended to introduce recent arrivals to the OPSEC concerns related to the missions and operating surroundings of their new commands. Also, semiannual follow-on training is conducted. This focuses on OPSEC concerns related to the specialty area or discipline in which the member is employed. Group seminars prove most worthwhile in follow-on training, because they allow members of like specialty areas to discuss OPSEC vulnerabilities. They are then able to devise measures to eliminate or control those vulnerabilities.

c. OPSEC training should be continuing and progressive. This should be the case throughout a service member's career. To this end, OPSEC training will include the following:

(1) OPSEC indoctrination briefing shall be given to all personnel. This shall occur within 60 days of arrival.

(2) Follow-up OPSEC training shall be conducted on at least a semiannual basis.

(3) Specialized training in OPSEC planning methods shall be given. All principal originators and consumers of operations planning guidance should attend.

d. A commander is responsible for what his unit does or fails to do. Obviously, OPSEC is no exception. With proper training and knowledge of what OPSEC is, the soldier will prevent valuable information from getting into the wrong hands. The old adage of "Loose Lips Sink Ships," is a very appropriate message when you are dealing with OPSEC.

THIS PAGE INTENTIONALLY LEFT BLANK

LESSON 1

PRACTICE EXERCISE

REQUIREMENT. The following questions are multiple choice. You are to select the one that is correct. Indicate your choice by CIRCLING the letter beside the correct choice directly on the page. This is a self-graded lesson exercise. Do not look up the correct answer from the lesson solution sheet until you have finished. To do so will endanger your ability to learn this material. Also, your final examination score will tend to be lower than if you had not followed this recommendation.

1. What is the technique used to determine the degree of security afforded to a given operation or function?

A. OPSEC program.
B. SIGSEC.
C. OPSEC survey.
D. COMSEC.

2. The task of determining the sensitive aspects of an operation (OPSEC) is the joint effort of which of the following?

A. S3 and S2.
B. S3 and S1.
C. S2 and S1.
D. S2 and S4.

3. One of the most important items to remember concerning OPSEC training is that it should be which of the following?

A. Continuing and progressive throughout a service member's career.
B. Conducted once and then forgotten.
C. Conducted at least every 3 years.
D. None of the above.

4. A program used to deny information to the enemy is called which of the following?

A. HUMINT.
B. OPSEC.
C. SIGINT.
D. REMS.

5. The most important source of information during wartime is usually which of the following?

A. Soldiers.
B. Refugees.
C. Enemy equipment.
D. Airplanes.

LESSON 1

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

Item		Correct Answer and Feedback
1.	C.	OPSEC Survey An OPSEC survey... (page 1-6, para 10d(1))
2.	A.	S3 and S2. Determine the... (page 1-5, para 10a(2))
3.	A.	Continuing and progressive throughout a service... OPSEC training should... (page 1-7, para 11c)
4.	B.	OPSEC OPSEC is designed... (page 1-1, para 1b)
5.	A.	Soldiers. However, the individual... (page 1-3, para 3a)

LESSON 2

IDENTIFY PERSONNEL ID AND CONTROL PROCEDURES

Critical Task: 191-386-0006

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn to identify and implement methods of personnel identification and control procedures.

TERMINAL LEARNING OBJECTIVE:

ACTION: Identify methods of personnel identification and control.

CONDITION: You will have this subcourse, paper, and pencil.

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

REFERENCES: The material contained in this lesson was derived from the following publications: FM 19-30, AR 600-8-14, AR 380-67, and AR 50-5.

INTRODUCTION

Perimeter barriers and protective lighting are physical security safeguards, but these alone are not enough. Security personnel daily see thousands of persons and property items. These move through security defenses all the time. There must be control of anything moving on and off post and restricted areas. Such control is critical. Several elements add to the effectiveness of any security system. Some of these elements are entry control rosters, personal recognition and ID badges and cards. Other elements are badge exchange procedures and personnel escorts. The best control occurs when the system uses all these elements. Simple, workable ID and control procedures should be used. This will make it possible to reach goals without impeding efficient post operations. Any good security system should be well organized and run: a personnel ID and movement control system provides not only a means of identifying those authorized to enter or leave an area but also provides a means of detecting unauthorized persons who try to enter. These goals are achieved by the following procedures:

- Determine who has a need to be in the area.
- Limit entry to those persons who have a right and need to be there.

- o Set up procedures for positive ID of persons within, and of persons authorized entry into, areas.
- o Issue special passes or badges to personnel authorized entry into restricted areas.
- o Use entry control rosters.
- o Use identification codes.
- o Use duress codes.

An additional purpose of control is to prevent entry of harmful devices, material, or components. It also limits theft or compromise of materiel or recorded information. A personnel ID and movement control system is the CO's most effective tool in a physical security program.

1. Means of Identification and Control of Personnel.

a. Screening of Employees. Screening of job applicants and employees is important in peacetime, and it is vital in time of a national emergency. Screening policies should be in standard personnel policies for peacetime and for times of emergency.

b. Personnel Security Questionnaire. A personnel security questionnaire is vital in the investigation of applicants and employees. The questionnaire should be checked for completeness. Drop obviously undesirable applicants from further consideration. A careful investigation should assure that the employee's character and associations are acceptable.

c. Sources for Data. Certain sources may be of aid in getting employment investigative data. A list of these sources follows.

(1) State and local police.

(2) Former employers.

(3) References (including those not furnished by applicant or employee).

(4) Public records.

(5) Credit agencies.

(6) Schools (all levels).

d. You may need to request data from any of the above sources. If so, insure you properly identify the applicant or employee. You should be aware of the antiscreening prohibition. This is covered under the Fair Employment Practices Act (FEPA) in some states. Privacy Act restrictions may also apply.

2. Personnel Clearances.

a. AR 380-67 outlines the policy and general procedure concerning security clearances to DA personnel. These clearances grant access to classified defense information.

b. The national personnel security program has one main purpose. That is to identify persons with beliefs or character dangerous to national security. It provides for a denial of, or removal from, positions of trust. Undesirables in position of trust could harm national interests. Positive evaluation of all persons must be made. Such assessment must occur before they are entrusted with sensitive data.

c. After the required clearance, the post CO issues a written order. In it, he states that a pass or badge be issued for entry to the appropriate area. The pass or badge will NOT indicate by word, color, or code the security clearance granted. No other document verifying a clearance is issued to a person. One should understand that a clearance shows that he is an acceptable risk: this has been determined by background investigations and national agency checks (NAC). It does not show that there is no risk at all. The "need to know" must still be the controlling factor.

3. Identification System.

a. Set up an ID and control system at each post or facility. This provides a means of identifying all military, civilian employees, and visitors. The system provides for the use of ID cards or badges. These aid in the control of movement of personnel into, within, and out of specified areas. The standard ID card is DD Form 2A (military) or DA Form 1602 (civilian employee). Either may be used for entry to areas which are basically administrative in nature. However, the post CO must approve this. These ID cards may be used in areas with no security interest. Persons needing entry to restricted areas should be issued a special security ID card or badge. These are shown in AR 600-8-14. The ID card or badge should be designed as simply as possible. Yet, they should still provide for a workable and adequate control of personnel movement.

b. Use the following guidelines in your pass or badge control system:

(1) Designate areas where passes and badges are needed.

(2) Describe pass or badge in use; describe the authorization and limitations placed upon the holder.

(3) Detail procedures at times of entry and exit, including nonoperational hours.

(4) Describe where, when, and how a pass or badge should be worn.

(5) Set up steps to be followed in case of loss or damage to a pass or badge.

(6) Set up steps for the disposition of ID media. This need may occur on termination of employment and actions as a result of security investigation and flagging actions.

4. Purpose and Scope.

a. A personnel ID system is established for security reasons to accomplish the following:

(1) Provide for the controlled entry of personnel into posts and facilities.

(2) Provide a practical system of positive ID of personnel with authorized entry to restricted areas.

(3) Aid the control of and circulation of personnel into, within, and out of restricted areas.

(4) Provide a visible means of easily seeing any limitations of personnel movement or access within restricted areas.

b. Security ID cards and badges are issued where a system of personnel ID and control is needed. They are used in addition to that control provided by the standard ID card. Security cards and badges will be used before movement into, within, and out of specified posts. Specified activities or restricted areas will also be covered by this system. Security ID badges in a limited area should undergo reissue when the loss factor reaches 5 percent.

5. Responsibilities.

a. Major COs and/or heads of Army staff agencies decide the use of security ID cards or badges. They decide also on withdrawal or reissue of cards and badges.

b. Major COs and heads of Army staff agencies are responsible for procurement (except for DD or DA forms) of these cards and badges. Preparation, issue, and use of completed ID cards and badges are also the responsibility of these persons. They are to enforce their policy on the use of such cards and badges as a security measure. Such responsibility may be delegated to COs where appropriate.

c. Major COs and heads of Army staff agencies must handle necessary budgeting and funding for ID cards and badges. The only exceptions are the DD and DA forms. Such responsibility may be delegated to COs where appropriate.

d. Major COs and heads of Army staff agencies may add other security features to the design of ID cards or badges. However, they must meet the specific security requirements in AR 640-3.

6. Specifications.

a. Security cards and badges may be photographic or non-photographic; they may be laminated, embossed, sealed, or otherwise joined to achieve the desired level of tamper resistance required by the installation or activity concerned. They will meet or exceed the specifications listed below:

(1) Must identify the name of the installation or activity for which the card or badge is valid.

(2) Must show the name of the person to whom issued. Visitor cards and badges may show "VISITOR" in place of name.

(3) Cards and badges must contain a card or badge serial number or sequence number to aid control and accountability.

(4) Cards and badges will show an expiration date.

(5) Cards and badges will identify the areas for which the card or badge is valid.

(6) Area designation may be visually shown on the card or badge or it may be coded by mechanical, electronic, magnetic, or some other method suitable to the desired level of security.

(7) All non-standardized cards and badges proposing the use of mechanical electronic, or other technological readers to determine access authorization will be approved by the MACOM before use.

b. The design of the security ID cards and badges must meet or exceed the following criteria:

(1) When a photograph is used, it should measure 1-inch wide and 1 5/16 inches in height. The photograph would eliminate the necessity to state descriptive data.

(2) Physical features which aid in identification may be listed. For example, height, weight, color hair, eyes, sex, date of birth, and fingerprints.

(3) The card or badge may show the name, grade, title, and signature of the authorizing official.

(4) If the card or badge has paper elements, the paper may be uniquely constructed, may portray a unique design or distinctive water mark or other features that make duplication or alteration difficult.

(5) The card or badge may contain design features difficult to duplicate such as visible cross threads or wires, fluorescent inks, and so forth.

7. Classification, Storage, and Control.

a. Control procedures should be set up. This should cover the issue, turn-in, recovery, or expiration of security ID cards and badges.

b. The engraved plates and all printed or coded component elements of the ID card or badge assembly should be handled as if they were "CONFIDENTIAL." They should be stored, safeguarded, and accounted for as required by AR 380-5. The source of ID cards and badges should be controlled. This will prevent use by unauthorized persons.

c. Sometimes cards or badges are damaged. These may come from discharged or transferred persons, or those whose employment has been ended. These cards or badges should be treated as "CONFIDENTIAL." They should be destroyed in accordance with AR 380-5 and other like regulations. Lost badges should at once be invalidated.

d. Immediately investigate the events surrounding a lost badge. It should be determined if the system has been compromised.

e. Security clearances will not be recorded on ID cards or badges.

f. Sometimes, ID cards or badges are lost through carelessness or negligence. If so, COs should provide for disciplinary actions.

8. Methods of Control.

a. Use of Escorts. The time will come when a person's name is not on the entry control roster at a restricted area or post. When this occurs, he must be escorted from the entrance to his destination. Persons listed on the entry control roster may be admitted without escort. This depends upon local policy. Escort personnel may be MPs, civilian guards, or representatives of the person visited. Carefully select escort personnel. This will insure their ability to properly perform escort tasks.

b. Personal Recognition System. This is the surest method of establishing positive ID. This system should be used with an entry control roster. The two will be used to admit and control the movement of unit or post personnel within a restricted area. This system is used when the area employs less than 30 persons per shift, and they are personally known to the guards. Also, these should be persons who are subject to a low rate of turnover.

c. Entry Control Roster. Admission of unit or post personnel to restricted areas should be granted only to those who are positively identified. Their names should appear on a properly authenticated entry control roster. They must be persons authorized by competent authority to enter. These rosters should be kept at entry control points to assure positive control. They should be kept current, verified and authenticated. They should be accounted for by a person designated by the CO. Admission of persons not on the roster should be first approved by the unit or post CO.

His designated representative may also give approval. Such persons will be escorted or supervised at all times while in restricted areas. Entry control rosters sent to a higher or lower level must be secured in transit. They must also be verified and authenticated upon receipt.

9. Badge Identification System.

a. A security ID card or badge system should be established to admit and control movement of everyone admitted to restricted areas. Three of the most commonly used systems are the single card or badge; card or badge exchange; and multiple cards or badges. These systems may require cards being carried on the person or cards or badges being worn on outer clothing. There are advantages and disadvantages of each type system. Security personnel must be aware of both.

(1) Single Card or Badge System. With this system, permission to enter different areas is shown on the card by letters, numerals, or colors. For instance, blue may be the background color of the card currently used for general admittance. Permission to enter specific areas of higher restriction may be designated by specified symbols or colors. These are overprinted on the card or badge. This system gives comparatively loose control and is not recommended for security areas. Permission to enter does not necessarily mean that one has the "need to know." Cards and badges often remain in the bearer's possession during off duty or off post hours. This increases the opportunity for alteration or duplication.

(2) Card or Badge Exchange System. This is a system of two cards or badges. Each contains identical photographs, but each has different background colors, or an overprint on one of the two. One type is presented at the entrance and exchanged for the other. This second type is carried or worn while in the area. It is identical in every way to the first with one exception. Additional symbols or colors have been added which grant further admittance. The polaroid camera with a special adapter can make up to four prints of one picture. This method provides extra security by having both photographs identical. In this type of system, the second badge or card is kept in the security area and never leaves. This decreases the possibility of forgery or alteration.

(3) Multiple Card or Badge System. This is a further development of the exchange system explained in paragraph (2) above with one exception. The card or badge does not have specific markings denoting permission to enter various restricted areas. Instead, an exchange is made at the entrance of each security area within the post. Exchange cards or badges are kept at each area only for those persons who have the appropriate card or badge. By virtue of the localized and controlled exchange requirements, this is the most secure and effective system.

b. In some cases a system of personnel ID and control other than personal recognition is in effect. Then, all persons are required to wear the ID badge. It should be worn in a visible place on the uniform; the location will

be prescribed by the CO concerned. Persons should be told that the security ID badge will not be shown off post.

10. Enforcement Measures.

a. The most vulnerable link in any ID system is its enforcement. Poor performance of duty by the security police in comparing the bearer with the card or badge may destroy the best system. Positive enforcement measures should be prescribed. These will insure effective operation of the ID and control system.

b. Choose security persons for duty at entrance control points carefully. Select them for their alertness, quick perception, tact, and good judgment.

c. Formalized standard procedures are a must for conducting guard mount and posting. Such steps are also necessary for relief of security persons. Frequent inspection of persons on post (conducted at irregular times) is effective. This prevents the posting of unqualified personnel and poor duty performance.

d. Establish a uniform method of handling or wearing ID cards or badges. If carried on the person, the card must be removed from the wallet or other container and handed to security police. A badge should be worn in a visible position. This will speed inspection and recognition from a distance.

e. Entrances and exits of restricted areas should be arranged in a certain way. Persons should be forced by this arrangement to pass in a single file in front of the security police. Turnstiles may be used to help maintain positive control of entrances and exits.

f. Artificial lighting at control points should illuminate personnel coming and going. It should be bright enough to enable the security police to compare and identify the bearer with the card or badge.

g. Card and badge racks or containers used at control points should be available only to security persons.

11. Custodial Responsibilities. A custodian must be named to accomplish control procedures. Basic control must include issue, turn-in, recovery, and expiration of badges or cards. The degree of compromise tolerable in the ID system is in direct proportion to the degree of security required or indicated. The following controls are recommended for the card and badge system:

a. Maintain an accurate written record or log. List, by serial number, all cards and badges on hand. Include to whom these were issued, and whether cards and badges are lost and/or destroyed.

b. Have custodian authenticate records and logs.

c. Have commissioned officer perform a periodic inventory of records.

d. Invalidate lost cards and badges.

e. Post current lists of lost or invalidated passes and badges at entry control points.

f. Set up controls to enable security persons on duty to determine the number of personnel within the area at any time. Security should be able to make this determination promptly and accurately.

g. Establish the two-man rule where needed.

h. Set up procedures to control movement of visitors to security areas. A visitor control record should be maintained, and it should be located where positive controls can be exercised.

12. Two-Person Rule.

a. The two-person rule is an additional security measure. It insures that no one person will have access to nuclear or chemical weapons. The rule requires the presence of at least two authorized persons. Each can detect incorrect or unauthorized procedures with respect to the task to be done. Each is familiar with applicable safety and security requirements. Also, each person will be present during any operation that affords access to sensitive weapons.

b. There are other areas where the two-person concept can be used in physical security. These areas include the following:

(1) Those areas where intentional or unintentional damage to equipment, machinery, or material must be prevented.

(2) Areas where uncontrolled access to funds must be prevented.

(3) Areas where uncontrolled access to arms and ammunition must be prevented.

(4) Areas where uncontrolled delivery or receipt of materials must be prevented.

13. Visitor Control Procedures.

a. A visitor is any person not listed on the entry control roster for that area. "Any person" includes post personnel.

b. Precautions against theft, espionage, and sabotage require special treatment. This includes screening, identification and control of visitors. Visitors to posts are generally in the following categories:

(1) Persons with whom every post must have dealings. Such would occur in connection with the conduct of its business. Examples are representatives of suppliers and customers, licensors or licensees, insurance

inspectors or adjusters, government inspectors at national, state, and local levels, service industry representatives, contractors, employees, etc.

(2) Sometimes individuals or groups just want to visit a post, and their purpose is not essential to operations. Such visits may be desired by business, educational, technical, or scientific groups. Persons or groups wishing to further their particular interest may also request entry.

(3) Individuals or groups are often sponsored by government agencies. Requests for visits by foreign nationals should be processed in accordance with AR 380-25.

(4) Some individuals and groups the government generally encourages. This is because of the contributions they make to economic and technical progress. The groups also aid defense production in the US and/or in friendly nations.

(5) Guided tours visit selected portions of posts in the interest of public relations.

c. The government tries to exclude from the US certain foreign nationals. These are those whose backgrounds indicate they might engage in espionage or sabotage. The government excludes them through visa, immigration, naturalization and related procedures. A foreign national issued an entrance visa or admitted to the US should not be considered free of security problems.

d. Arrangements for the ID and control of visitors may include the following:

(1) Positive ways of establishing the authority for admitting visitors. Limitations relative to entry should be established.

(2) Positive ID of visitors by personal recognition, visitor permit, or other credentials. The employer, supervisor, or office in charge should be contacted. They can determine the validity of the visit.

(3) Availability and use of visitor registration forms and records. These provide a record of identity of the visitor. Such logs also record the time and duration of the visit, and other important control data.

(4) Availability and use of visitor cards or badges. These should be numbered serially. They should indicate as much of the following information as possible.

(a) Bearer's name, or visitor.

(b) Area or areas to which entry is authorized.

(c) Escort requirements, if any.

(d) Expiration date.

(5) Procedures which will insure supporting personal ID plus checking of visitor cards or badges at restricted area entrances.

(6) Procedures for escorting visitors through areas where an uncontrolled person could acquire unauthorized data. Foreign national visitors should be escorted at all times.

(7) Controls which will recover visitor cards or badges on expiration, or when no longer required.

(8) Twenty-four hours advance approval when possible. Where needed, the post should prepare a schedule for the visit, and the post should designate an escort officer.

e. Enforcement of the ID and control system rests with post security persons. It is a must that they have the full cooperation of employees. These should be educated, and they should be encouraged to assume this responsibility. They should also be instructed to consider each unidentified or improperly identified person as a trespasser. In some restricted areas passes are limited to certain zones. In these cases, employees should report movement of person to unauthorized zones.

14. Control Movement of Employees After Hours. A system should be kept for the control of personnel after hours. The guard force can then record their departure time. Often, persons may have valid reasons for staying later. The person, however, may be involved with some illegal act not readily apparent. By recording the name, departure time, and badge number, if available, a permanent record can be established. The person could be questioned at a later time if anything happened on the post during the time they remained late. No person should be allowed admittance to re-enter a restricted or sensitive area without proper authorization. This can be oral or written. Officially designated persons of the post grant this authorization.

15. Special Safeguards.

a. Signs/Countersigns and Code Words. Sign/countersign systems and code words may be used in certain security areas. Proper safeguards must be established to ensure constant checking and testing of the systems. This will assure immediate change when the sign/countersign or code word is compromised. Sometimes more controls are required. If so, the security management system or security police orders should provide instructions.

b. Duress Code. This is a word or phrase which can be fitted into normal conversation. It is used when guards or other personnel are forced to vouch for unauthorized persons. The aim of these persons is to gain entry to a security area. When such a system is used, you must ensure immediate support; any security person giving or receiving the signal must receive prompt aid. The duress code should be simple, and it must be changed often to lessen the chances of its compromise.

16. Photographs. Photographs are sometimes taken within a restricted area. If so, the photographer should be cleared for access, and he should be escorted at all times. Actual taking of photographs should be under the supervision of intelligence or protective personnel. This will ensure that classified data does not accidentally appear in the pictures. Each negative should be secured until its first print has been carefully examined. Examiners should be particularly alert to backgrounds. Small parts of a picture might reveal classified data if enlarged.

17. Contractor Employee. Contractors usually know their key personnel. However, it often happens that most of the employees are short time laborers. They are unknown to their employer. On a construction job a large number of men will be involved over a period of time. It is then advisable to fence off the construction area from the rest of the post. Where the contract work is infrequent and for short periods of time, security may be more economical. Each case will have to be considered separately. A decision should be made based on the physical layout and the sensitivity of the post. It is advisable to make local background checks on contractor personnel.

18. Utility and Maintenance Personnel. No group of occupations has been used as well and as often as a cover for unauthorized entry as this one. Correct clothing, a toolbox, and a bit of technical knowledge are the only requirements. These people can pose as telephone repairmen, electricians or plumbers. They can pose as business machine maintenance people. Cleaning persons for government offices and buildings make excellent covers for espionage and sabotage. Current espionage cases have revolved around this type of cover-up. Legitimate employees of public utilities and some commercial service companies usually carry company ID. They should, however, not be admitted to a restricted area without at least a telephone check. This can be made to their home office to establish their authenticity. Also, these persons should not be admitted without a check with the person who requested their service. Movement within the post should be subject to the same pass and escort procedures as prescribed for other visitors. Such would be the case during duty or off duty hours.

LESSON 2

PRACTICE EXERCISE

REQUIREMENT: The following questions are multiple choice. You are to select the one that is correct. Indicate your choice by CIRCLING the letter beside the correct choice directly on the page. This is a self-graded lesson exercise. Do not look up the correct answer from the lesson solution sheet until you have finished. To do so will endanger your ability to learn this material. Also, your final examination score will tend to be lower than if you had not followed this recommendation.

1. When an employee is granted a clearance, it is an indication that the employee is which of the following?

A. To be allowed access to all TOP SECRET material.
B. Absolutely loyal to the country.
C. An acceptable security risk.
D. No longer a security risk.

2. What is a proper procedure for taking publicity photographs on the installation?

A. Allow unrestricted processing and printing of films.
B. Require re-examinations of the negatives by security personnel every time more prints are made.
C. Require security or intelligence personnel to supervise photography to avoid revealing classified data.
D. Allow photographers unrestricted picture taking in order to promote public relations.

3. The two-person rule is an additional security measure. What is it designed to do?

A. Ensure you have someone to talk to while working.
B. Ensure that no one person will have access to nuclear or chemical weapons.
C. Ensure that you will not go to sleep while on the job.
D. All of the above are correct.

4. Area K has 50 employees; Area L, 43 employees; Area M, 28 employees; and Area Z, 21 employees. The personnel recognition system could properly be used in which areas?

A. M and Z only.
B. L and Z only.
C. K and M only.
D. Z only.

5. What is the most vulnerable link in any badge system?

A. Theft of a badge by an outsider.
B. Enforcement of the system by entry control personnel.
C. Loss of a badge by an employee.
D. Mutilation of a badge by anyone.

6. Which of the following BEST describes the purpose of an ID and control system?

A. Limit only civilian personnel who are cleared, have a need to know, and are employed in the area.
B. Limit entry to all vehicles, except emergency vehicles such as police cars, ambulances, and firetrucks.
C. Assure a check of badges of all employees is made and all violations are reported.
D. Assure a means of positive ID of all personnel who are authorized entry to an area.

7. Security ID cards and badges should be tamperproof. They will meet the requirements of:

A. AR 380-13.
B. AR 200-16.
C. AR 640-3.
D. AR 380-25.

8. Which of the following is a proper action to take in setting up a badge control system?

A. Have each activity on the post responsible for making and issuing its badges.
B. Prepare only one badge for each person so a duplicate will not be in existence.
C. Place a security classification on civilian badges to assure handling as a classified document.
D. Establish centralized control of badges.

9. ID badges for visitors must contain, at least, name of activity for which it's valid, a serial number and signature of validating official. These badges must also contain what else?

A. A letter, symbol, or color to indicate access authorized.
B. A photograph and visitor's signature.
C. Escort requirements and photograph.
D. Letter, symbol, or color to indicate access authorized, and expiration date.

10. Entrances and exits of restricted areas should be arranged so coming and going personnel are forced to do which of the following?

A. Pass in single file in front of the security police.
B. Show their badges to the security police.
C. Pass in front of the guard two at a time.
D. All of the above are correct.

11. After the required clearance and written order of the post CO, a pass or badge is issued for entry to the appropriate area. The pass or badge will NOT indicate which of the following?

A. Age, race, or birthday.
B. Sex, age, or birthday.
C. Indicate by word, color, or code the security clearance granted.
D. None of the above is correct.

LESSON 2

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

Item		Correct Answer and Feedback
1.	C.	An acceptable security risk. One should understand... (page 2-3, para 2c)
2.	C.	Require security or intelligence personnel to supervise... Actual taking of... (page 2-12, para 16)
3.	B.	Ensure that no single person will have access to nuclear... It ensures that... (page 2-9, para 12a)
4.	A.	M and Z only. This system is used... (page 2-6, para 8b)
5.	B.	Enforcement of the system by entry control... The most vulnerable... (page 2-8, para 10a)
6.	D.	Assure a means of positive ID for all personnel... Provide a practical... (page 2-4, para 4a(2))
7.	C.	AR 640-3. However, they must... (page 2-4, para 5d)
8.	D.	Establish centralized control of badges. Control procedures... (page 2-6, para 7a)
9.	D.	Letter, symbol, or color to indicate access... Identify the post... (page 2-5, para 6a(4) and (8))
10.	A.	Pass in single file in front of the Persons should be... (page 2-9, para 10e)
11.	C.	Indicate by word, color, or code the security... Security clearances will... (page 2-6, para 7e)

LESSON 3

DETERMINE BOMB THREAT CONTINGENCY PLANNING

Critical Task: 191-386-0012

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn to supervise planning, expectation, and securing phases regarding bomb threats.

TERMINAL LEARNING OBJECTIVE:

ACTION: Supervise planning, expectation, and securing phases of bomb threats.

CONDITIONS: You will have this subcourse, paper and pencil.

STANDARDS: To demonstrate competency of this task you must achieve a minimum score of 70 percent on the final subcourse examination.

REFERENCES: The material contained in this lesson was derived from the following publications: FM 19-30, FC 19-106, and TC 19-5.

INTRODUCTION

Bomb threats present serious potential danger to an activity or post. The motives, targets and bombers, themselves, are diversified. Due to this fact, bomb threat planning and training is an important part of any physical security program. Physical security personnel must develop an awareness of the serious nature of bomb threats; they must understand preplanning considerations and how to prepare a bomb threat plan. They must understand actions to take during an after receipt of a threat. They must also understand the various responsibilities relative to bomb threats. Your office telephone rings and the voice on the other end says..."A bomb is going to explode..etc., etc..." Would you know how to respond? As the physical security officer, once you are notified of such a call, would you know what to do? Contingency planning and training would prepare you for handling the incident.

1. Definitions.

a. Bomb. A bomb, when detonated or ignited, is a device that can cause damage to material and injury or death to personnel. Bombs are classified as explosives or incendiary. An explosive bomb causes damage by fragmentation,

heat, and blast wave. The heat produced often causes a secondary incendiary effect. An incendiary bomb generates fire-producing heat; it does not cause a large explosion when ignited.

b. Bombing. A bombing occurs when an explosive bomb detonates, or an incendiary bomb ignites.

c. Bomb Threat. A bomb threat is a message delivered by any means; it will warn or claim the presence of one or more bombs. A bomb threat may, or may not, specify the location of a bomb; it may, or may not, contain an ultimatum related to the detonation/ignition or concealment of the bomb.

d. Bomb Incident. This is any event involving the detonation or ignition of a bomb. It can also be the discovery of a bomb, or the execution of a bomb threat.

e. Bomb-Incident-Preventive Measures. These are measures taken to reduce the production and placement of bombs. Measures are also meant to reduce the disruptive effect of bomb threats.

f. Bomb Threat Plan. This is a complete plan which assigns responsibilities and specific actions to be taken when a bomb threat or bombing occurs.

2. The Bomber.

a. Psychology. Developing a psychological profile of persons capable of such anti-social behavior is nearly impossible, since bombers have come from all walks of life. Also, they have come from various age groups and differing economic and social backgrounds. Many bombers are known to be deranged and/or have character disorders.

b. Technology.

(1) The popular idea of a bomb is a black sphere the size of a bowling ball, equipped with a sputtering fuse. This is not likely to be encountered in sabotage by explosion. An explosive bomb itself is the unit of destruction and it is not dependent upon outside aid as is an incendiary bomb. Because of these traits, an explosive bomb is normally larger than an incendiary bomb. However, the same ingenuity of disguise is applicable. Five sticks of dynamite taped together and equipped with a blasting cap would make a capable bomb, but upon sight, this would cause suspicion and concern. The same five sticks of dynamite stuffed in a suitcase with a dry cell battery and a clockwork delay device would be just as destructive, but it would not attract attention. A lump of plastic explosive coated with a mixture of shellac and coal dust would be unnoticed in a load of coal. The possible combinations of explosive, activator, delay device, and outside container are many.

(a) Most high school chemistry courses provide enough knowledge to enable a person to make a bomb.

(b) Common household items readily available may be treated and assembled as an effective explosive device. Other items for making bombs are used widely in mining, agriculture, and some industry. Also, they are not hard to produce.

(2) Common Explosives. Bombs are classified according to the time it takes common explosives to burn or detonate. They are either low explosives or high explosives. The slower acting low explosives have a pushing effect in action, whereas high explosives have a shattering effect.

(a) Low Explosives.

1. Black powder is the oldest known explosive, but its use has declined. This is due to the development of more efficient explosives. Black powder is granular, and the size of the grains varies for different uses. In appearance, it is shiny black, and in burning gives off a heavy white smoke. It burns freely in the open air, and it must be confined for an explosive effect. It is used in pipe bombs and other improvised devices.

2. Smokeless powder is not a powder, and it is only smokeless in comparison to black powder. It is made by treating plant fibers (cotton or wood) with nitric and sulfuric acids to form nitrocellulose. It may be used in pipe bombs and similar devices in the same way as black powder. Generally, this powder has a more powerful effect.

(b) High Explosives.

1. Nitroglycerin is an oily, colorless liquid that explodes violently. However, due to its sensitivity to shock, it is not widely used in its liquid state. When combined with other materials, it loses its sensitivity. It is made into dynamite and plastic explosives.

2. Dynamite is the most widely used commercial explosive. (In the military it may be classified as a low explosive.) Basically, it is nitroglycerin absorbed in a porous or absorbent material, such as sawdust. The percentage of nitroglycerin varies, and other ingredients are added to fit the intended use. It is packed in sticks, usually round, and covered with paraffin impregnated paper. The strength is marked on the outside of the wrapper. A blasting cap detonator is necessary to cause an explosion. Sometimes dynamite is stored in one position for a long period, however. If this is the case, the nitroglycerin tends to seep to the lower side and becomes sensitive. Dynamite is convenient, available, and effective. These qualities make it a favorite explosive for the saboteur. The high velocity of its explosion makes it unnecessary to confine it to make an effective bomb.

3. Trinitrotoluene (TNT) is a yellow solid, usually formed into blocks of various sizes. It is insensitive to shock, easy to handle, and has powerful explosive properties. Because of this, TNT is excellent for sabotage purposes.

4. Nitrostarch is also a good explosive for sabotage for the same reasons as TNT. It is slightly less powerful than TNT, but it is more sensitive to flame, friction, and impact.

5. Compositions C3 and C4 are yellow and white respectively, and are odorous and plastic. They have about the same sensitivity as TNT, but they are more powerful.

(3) Initiating Devices. There are two general types of initiating devices. One is that which produces flames (for use with low explosives). The other is that which detonates (for use with high explosives).

(a) Flame-Producing Devices.

1. A safety fuse consists of a powder core wrapped in paper or cloth fiber. It is usually waterproofed. It is the medium through which flame is conveyed for the direct or indirect firing of a low explosive. An example of direct firing is black powder. An example of indirect firing is the ignition of a blasting cap to detonate dynamite.

2. A miner's squib is a thin paper tube of powder sealed at one end with a wax plug; the other end contains a fuse or wick. The wax plug is pinched off at the time the squib is used. The fuse burns slowly, and when it reaches the powder, a flame shoots out the open end.

3. An electric squib consists of an aluminum tube one and one-half inches long with leg wires protruding from one end. When an electric current is applied to the leg wires, the firing element flashes. It then ruptures the tube and sends an intense flame into the explosive.

(b) Detonating Devices.

1. A blasting cap (nonelectric) is a small tube closed at one end and loaded with a charge of an explosive. It can be detonated by the spit or sparks from a safety fuse. Blasting caps are sensitive to shock, friction, and heat, and they are dangerous when not properly handled. For use, a length of safety fuse is inserted in the open end.

2. Electric blasting caps are similar in appearance to nonelectric caps, except that they are fired by electric current. They have the same sensitivity as nonelectric caps, and great care must be used in storing and handling them. They come in various numerically designated sizes; Number 8 is the one in common use.

3. Detonating fuse or cord is a fuse which has an explosive core. It requires a blasting cap to detonate, and the extreme violence of the action is enough to detonate a high explosive in contact with it. It is usually wrapped around or taped to the charge to be detonated. It is used for the simultaneous firing of a number of shots at some distance apart.

3. Bombing Targets. Targets chosen by bombers may be randomly or carefully selected. The psychological makeup, along with the motivation for bombings, are interrelating factors in determining targets. Any number of factors may isolate target selection. These factors include hatred, perceived unfair treatment, excitement, and anarchy. A list of potential bombing targets to be considered by security personnel follows. The list is not limited to these, however:

a. Residents.

b. Commercial operations.

c. Vehicles.

d. Schools.

e. Public safety buildings.

f. Persons.

g. Public buildings.

h. Military installations and activities.

i. Public communications facilities.

j. Public utilities.

4. Bombing Motives. Bomb cases of historical importance have generally been politically motivated. However, it would be a mistake to overlook the other possible motives. When devising preventive measures and bomb threat plans, remember two things. There are two basic categories of motives for bomb placement and threats: nonpolitical and political.

a. Personal animosity is often the motive behind many bombing incidents. The quest for vengeance results form being fired, perceived injustices, harassment or other psychological disorders. Any of these may be underlying factors.

b. Malicious destruction may account for the simple desire for power or excitement. Vengeance as well as other factors should also be considered.

c. Labor disputes often arouse attacks from either or both sides. Such attacks serve as a means of pressure in making gains in labor contract negotiations. Attacks are aimed at strike breakers. They are also aimed at non-union laborers as well as union and company officials.

d. Monetary gain, more commonly known as extortion, is the motive for bombings of large companies or rich businessmen.

e. Political bombings in recent decades have presented the most serious threat to society.

(1) Terrorists use bombings as a tool to call attention to and publicize their cause. They do so to show the weakness or helplessness of governments. They may do so to extort money, supplies, or the freeing of political prisoners. Bombing government offices destroys records and interrupts normal operations.

(2) Political bombings are psychological tools.

f. Civil rights disputes all over the US since the early sixties resulted in bombing attacks. These attacks took place on schools, churches, residents, and prominent persons.

5. Bomb Threat Planning Considerations.

a. Preventive Measures. As stated before, there are many motives and techniques used in bombings. Preventive measures, then, must provide useful guidance in a crisis and cover a variety of cases. The person responsible for the bomb threat plan must consider the three things needed for a successful bombing:

(a) Ability to make and detonate an explosive device.

(b) Access to raw materials or explosives.

(c) Opportunity to place the bomb at the desired target.

Special attention must be given to (c), because this is the one area in which a law enforcing organization has the best chance to discourage a bomb incident. Enough preventive measures and physical security precautions must be established. Then, the opportunity to obtain explosives and place bombs will be reduced. Also, a good bomb threat plan and a well-rehearsed procedure for handling them and incidents will reduce the chances of a bomb being detonated. See Appendix A for a sample format to be distributed and used to record valuable information relating to bomb threat calls. This documentation may provide clues and other useful data for security personnel.

b. Physical Security Measures. FM 19-30 presents a discussion of physical security measures. These measures may be used to limit the chance of this organization or facility experiencing a bomb threat. Such measures include but are not limited to the following:

(1) Having a workable personnel ID and control system.

(2) Having a package and material control system.

(3) Maintaining strict control of locks and keys.

(4) Having enough perimeter barrier and lighting systems.

(5) Locking doors to boiler rooms, basements, and utility closets when not in use.

(6) Eliminating places in which to hide a bomb by good housekeeping habits. Accumulated trash and discarded materials are examples of such places.

(7) Training employees to report strange people or packages.

c. Communications Channels. Establish channels so that Federal and local law enforcement agencies can send information about possible threats to your facility. Local law enforcement agencies will have access to the latest data from the FBI.

d. Support Organizations. Include the supporting Explosive Ordnance Disposal (EOD) Detachment and the local fire department. Both of these groups will provide help in developing bomb threat procedures. However, during a bomb threat, the duties and responsibilities of each are limited by regulation. The person preparing the bomb-threat plan should know these limitations.

e. Emergency Operations Center (EOC). The EOC should have access to both radio and telephone communications. They will use these when a bomb threat is received. The EOC may be the provost marshal's office but, this office may also be a prime target for a bomb threat. Therefore, an alternate EOC should be selected. Persons in the EOC should have the authority to decide on actions to be taken during a threat.

f. Inspections. Inspect buildings on a regular basis. This will reduce the possibility of a bomb being placed, and it will also lessen the time required for the search after a threat has been received. Inspections will reveal hiding places for bombs, possible targets, and building weaknesses. The inspector will become so familiar with his area that he should notice any new or strange item immediately. The inspector should be the supervisor in his area or a member of a predesignated search team.

g. Reporting System. People must know whom to notify, and how, in case of a bomb threat. Communication methods and procedures must be determined before, not after, a bomb threat is received. Telephones, whistles, and bullhorns are very important to communications during searches because of the possibility of detonating an electric blasting cap by radio transmission. Radios transmissions should not be used within 150 feet of the threatened area. This includes the small hand radios used by police and security persons. (Also sirens on emergency vehicles may not be used.)

h. Search Teams. There are three groups of persons who may serve as members of the search teams. They are building supervisors, building occupants, and special search teams. The trained search teams are the most effective. This is especially true when they are combined with a brief search by occupants before evacuation.

6. Preparing the Bomb Threat Plan.

a. The main goal of a bomb threat plan is to minimize injury to personnel, damage to property, and to avoid disrupting operations. Another goal of a bomb threat plan is to take those steps which will improve chances of catching the offenders. Bomb threat plans are also bomb incident preventive measures, because bomb threat plans reduce damage and disruption. They also aid in catching offenders. As a minimum, the bomb threat plan should provide guidance for the activities listed below:

(1) Control of the operation.

(2) Evacuation.

(3) Search.

(4) Finding the bomb or suspected bomb.

(5) Disposal.

(6) Detonation and damage control.

(7) Control of publicity.

(8) After-action report.

b. In setting up these operations, the person or group responsible for a particular job should be appointed, notified, and well-trained and rehearsed in actions to be taken. The person preparing the bomb threat plan should ask and answer questions about each area of operation.

(1) Control of the Operation.

(a) Who will be in charge of the incident? In the Army this is a command decision. The CO or his designated representative is in charge. He is the Bomb Scene Officer, and he should have all available training in this subject area.

(b) Where will the command center be located? To whom and how will the threat be reported? This should be decided by each unit so that everyone will know where to report and how to locate the CO or Bomb Scene Officer.

(c) How will critical decisions be made? These should be made by the CO or his Bomb Scene Officer.

(d) Who will man the control center? Decisions should be made by the CO or Bomb Scene Officer, communications personnel, engineer, or public affairs officer.

(2) Evacuation. Moving a large number of people under emergency conditions is dangerous unless absolute control is maintained. So particular attention should be given to planning evacuation procedures. At first thought, immediate and total evacuation would seem to be the best response to any bomb threat; however, there are significant economic and safety factors that may weigh against the evacuation. Even where evacuation is possible and wanted, the process may not be as simple as it might appear.

(3) Search.

(a) Who searches? Except in the rarest cases, EOD and MPs will NOT be used to search for reported explosive devices in barracks, community areas, buildings, and offices. Rather, such searches will be done by designated persons familiar with the area and its contents. If an unusual item is found, EOD is to neutralize and evacuate the device for disposal. MPs are to be used around the threatened area to control traffic, and they are used to provide other regulatory services. (The preceding is a paraphrase of a current TRADOC letter which is still in effect.) Therefore, in the Army, the occupants of the building will perform the search along with designated search teams.

(b) What will be searched? Occupants will search their own work area and rooms. In addition to this, search teams should be assigned to search public areas, restrooms, and closets. Keys should be available to searchers so that every area can be reached. A complete search must be made, since one or more bombs could exist.

(c) When do you stop the search? Do so after the entire facility has been searched. Remember that the discovery of one device should not necessarily cause the search to be stopped; there could be more than one bomb.

(4) Actions Required When a Bomb or Suspected Bomb is Found.

(a) Any suspected incendiary device or bomb should not be touched or handled in any way by the search unit. The person in charge should contacts MPs. They will then notify the nearest military EOD Detachment. People have been disfigured and killed by trying to handle bombs for which they are not equipped or trained to do.

(b) EOD personnel will attempt "render safe" procedures.

(c) In case of an actual bombing, all persons are warned not to move the debris. It will be searched by government authorities for clues, and all foreign evidence will be removed for scientific analysis.

(5) Disposal. How will suspected bombs be processed? When a searcher finds a bomb, he should not touch the device. He should immediately clear the area and notify the emergency operations center. The EOC will then notify EOD to deactivate and remove the bomb. EOD will probably not respond to a bomb threat until a bomb or suspected bomb has actually been found.

Local policy may differ as to when EOD should respond; thus, this should be determined when the bomb threat plan is prepared.

(6) Detonation and Damage Control.

(a) What procedures will be taken if a bomb goes off without warning or during a search or disposal operation? During planning stages, damage control teams, first aid teams and heavy and light rescue teams are set up. Also, communication teams should be established. Damage control teams will go to the scene of the explosion and try to control any fires; they will remove flammable items and allow venting. They will also disconnect utilities, as needed, and have fire and medical teams stand by. Rescue teams will go to the scene to aid and evacuate any injured parties. First aid teams will report to the aid station and give first aid to the injured. Communication teams will set up communication between these first aid teams and the control center.

(b) How will utilities, transportation and other support services be obtained and used? The engineers should cut off power and gas to limit the possibility of fire in the area of the blast. The organizations or person(s) responsible for transportation and other support services must be designated in the bomb threat plan.

(c) The bomb threat plan should name the people assigned to the damage control team, light rescue team and heavy rescue team. It should also name the people on the litter team, first aid team, and communications team.

(d) If a bomb goes off, the major problems are the treatment of casualties and the control of any fires. In cases where a bomb search is in progress, fire and medical personnel and equipment should be on a standby basis. They should wait outside of the 300-foot evacuation radius.

(e) The possibility of more than one bomb should not be overlooked, and the remaining areas of any building or facility should be searched. This should be the case even though one explosion has occurred. Procedures for searching the detonation site for physical evidence should be followed as for any crime scene.

(7) Control of Publicity. The Public Affairs Officer is the only person who should release information to the press. All others should be told not to discuss the current situation with any outsiders, especially the news media. This control measure insures that more bomb threat calls are not brought on by statements from uninformed sources.

7. The Threat. A bomb threat may be received in many ways. A suspicious package may be sent through the mail; a written message may arrive, delivered through the mail or by messenger, or by telephone. The telephone message is the most often used method.

a. Telephone Messages.

(1) Chances are very small of receiving a warning call that a bomb has actually been placed. We cannot ignore telephone warnings because there have been cases where a threatening call was not a hoax.

(2) The person making such a call could reveal enough information about himself so that he might later be identified. There have been cases where a caller has not only described the bombing device, he has given its location, and stated the time it was to go off.

b. Actions to Take When Warning Call is Received (See Appendix A). It is not feasible to put telephone tracing and recording equipment on all lines on post; therefore, persons apt to receive such calls should be briefed on and trained in the following procedures:

(1) Try to keep the caller on the line long enough to trace the call and get more information.

(2) Record, in writing or by tape, the exact words of the caller. Try to find out the location of the bomb, the type of device, and what it looks like. Try to find out the expected time of detonation.

(3) Try to figure out the sex, approximate age, and mental attitude of the caller. Try to determine exactly his reasons or motives for placing the bomb.

(4) Note any background noise that may provide a clue to the caller's location.

(5) Note any accent or peculiarity of speech that may help to identify the caller.

(6) If time permits, ask the caller a question. Examples are, "Who is this calling, please?" "What is your name?" In some cases, the caller may unthinkingly reply.

c. After the Threatening Call. After the threat has been received, the person who took the call should promptly notify a predesignated person(s). This may be your supervisor, the Bomb Scene Officer, Staff Duty Officer, or the MP Desk Sergeant.

8. Evaluating the Threat.

a. Analyze the bomb threat immediately after it is received, to avoid dangerous delay and indecision. Person(s) must be predesignated to determine the following:

(1) How will the threat be evaluated?

(2) Who will evaluate the threat?

b. Evaluate the bomb threat, and take proper action by:

(1) Reporting the message to proper authorities in all cases.

(2) Search without evacuation (overt or covert).

(3) Evacuate and search.

c. Starting the Plan. When a bomb threat is received, the bomb threat plan should begin. It should have been so expertly planned and in such detail that it can be started simply by a call. The call will be made to a predesignated officer or activity, such as the Bomb Scene Officer. Or it may be made to the Staff Duty Officer or the MP Desk Sergeant.

d. The After-Action Report. A complete after-action report is essential to an investigation of a series of bomb threats. The report should be submitted as a Memorandum. A sample format is furnished in Appendix B.

9. Search Techniques.

a. General. There are many factors to consider before ordering a search, if you are the commander or Bomb Scene Officer:

(1) Will the search be overt or covert?

(2) Will the search be conducted before, after or without evacuation?

(3) Will the search be conducted by supervisors, occupants, or a special team?

(4) How much of the building will be searched?

A detailed search of even a medium-sized building can take from 12 to 24 hours, and moving the furniture and equipment around will cause a lot of confusion and inconvenience to the occupants. Many bombs are set off by some type of watch or-clock mechanism. Because of this, the lapse of time between setting the bomb and receiving the warning usually will leave less than 12 hours.

b. The extent of any search will be determined by the number of people on hand to search. The extent will also depend on the CO's evaluation of the threat. Remember, MPs do NOT order searches, evacuation, or re-entry into a building after an evacuation. These decisions are made by the CO, building supervisor concerned, or bomb scene officer. See Appendix C for a sample search checklist.

c. The person or group chosen to conduct the search must be given special training. This must cover systematic search procedures. They must be taught to recognize a bomb or explosive device (EOD will assist in this training). The key to a successful search is to be systematic. All searches must proceed in an orderly manner from the starting point throughout the area each room should be marked or sealed after it has been searched. Be certain

the team has plastic ribbon, string, or crepe paper for marking searched areas.

d. Equipment. Equip search teams with equipment such as screwdrivers (standard and phillip), crescent wrench, flashlight, and hand mirror. Each member should have body armor, such as a flak vest.

10. Search Techniques - Outside.

a. Search from the outside to the inside, and from the bottom to the top. This method has resulted from years of experience, and it reduces the risk of injury to both the searchers and the occupants.

b. Conduct all phases of the search at the same time, if a large, trained search team is available. If the search team is to be divided, use the following breakdown of team members:

(1) Outside search - 25 percent.

(2) Public areas - 25 percent.

(3) Detailed building search - 50 percent.

The smallest search unit should consist of two men because of the psychological and physical advantages. Two men will conduct a more thorough search, and they can work together when heavy furniture must be moved.

c. The search of the outside of buildings is more important, because these areas can generally be considered public areas with easy access to the bomber. This is especially true during the hours of darkness, when many buildings are closed. The outside search pattern begins at ground level. Close attention must be given to the following areas:

(1) Piles of leaves or refuse.

(2) Shrubbery.

(3) Entrances.

(4) Manholes.

(5) Trash cans.

(6) Parked vehicles (look only; must be searched by EOD personnel).

Search to a distance of 25 or 50 feet from the building, outward. After completing the ground-level search, return to the building. Search window ledges, air-conditioning units, signs, building ornamentation, fire escapes, and the roof. After completing the outside search, add members of this team to the inside search team (See figure 3-1).

11. Search Techniques - Inside.

a. Start the search of the inside in the basement and work toward the top floor. If a separate public area search team is organized, use building custodial personnel on the team, because they are most familiar with the area to be searched. Examples would include reception rooms, lobbies, elevators, stairs, custodial closets, and rest rooms. As search teams move throughout the building, mark each area as it is searched. One method of indicating a "search-completed" area is to tie a piece of string or crepe paper across the door opening.

b. When conducting a detailed room search be certain to follow these steps:

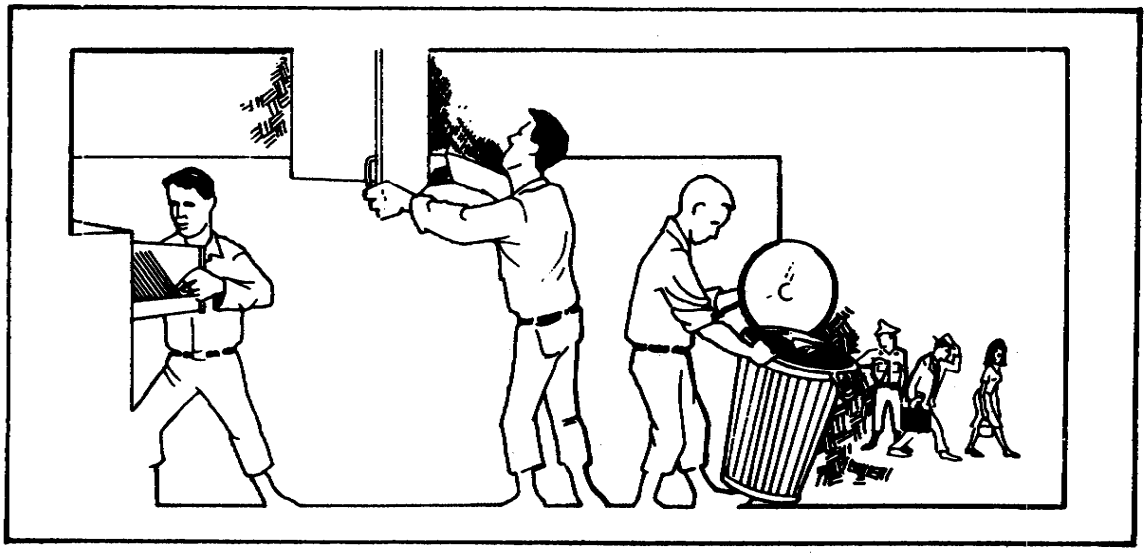


Figure 3-1. Search Techniques.

(1) Move into the room, stand with eyes closed, and listen. Often clockwork timing devices can be detected without special equipment.

(2) Divide the room into equal parts according to the number of objects to be searched, not the size of the room.

(3) The first sweep of the room includes a check of all objects from the floor to waist level. Include items built into the wall. This sweep will require the most time and effort, because it includes almost all items of furniture, and areas underneath rugs.

(4) The second sweep, in most cases, will include all items from waist to ceiling. Under some conditions, certain area may be left for a third sweep. These include false ceiling spaces, heating ducts, and indirect lighting fixtures.

(5) The room search is ended only when the person in charge is satisfied that an adequate search has been made. Remember the searcher should never say, "There is no bomb". He should only say, "No bomb was found."

12. Evacuation Procedures.

a. During evacuation, route people through the most public areas of the building (corridors and stairwells). Extreme CAUTION must be exercised to insure an orderly evacuation, since these are also the areas most likely to contain an explosive or incendiary device.

b. Set up routes and priorities based on the type of building and the location of people within. Assign and train persons to act as guides. These will lead the evacuation and control the people during exit.

c. Routes and priorities will also depend on the type of building and the location of people in relation to the area where the bomb is. In multistory buildings, rooms on floors above the danger point and immediately below should be evacuated first; also, on the same floor, evacuate three rooms away on all sides.

d. Before giving the order to evacuate, the CO should consider the following:

(1) The caller - what did he say? Did the caller sound serious in his threats?

(2) Has this been a recurring thing?

(3) Are employees excused from work when such threats are experienced?

(4) Is it possible that this call was brought about by news reports of other calls?

(5) Will immediate evacuation of the premises expose personnel to greater danger?

(6) What is the size of the building; how many people are involved?

13. Other Considerations. Other questions must be answered when preparing the bomb threat plan. These are as follows:

a. Who has the authority to order evacuation? The CO or building supervisor or bomb scene officer have the authority to order evacuation. MPs do NOT order evacuation.

b. Who makes the decision to permit re-entry into the building after a search in which no bomb is found? The Bomb Scene Officer in control of the operation. MPs do NOT order re-entry into a building.

c. How will evacuation be signaled? Establish a signal for evacuation and proceed according to the plan.

d. If evacuation is ordered, what procedures will be followed? Evacuation teams should be assigned to guide the occupants out of the area. Alternate evacuation routes must be provided, preferably the same routes used in case of fire.

e. Who will be part of the evacuation team? These people should be assigned before the incident and thoroughly trained. Areas through which evacuation will proceed should be searched and cleared before evacuation. These include areas inside and outside the threatened building. Public areas are the most likely places for a bomb to be located, and they are the usual avenues of exit. The evacuation team should be able to control evacuation and eliminate panic that could lead to injuries.

f. To what area do you evacuate the occupants? Occupants should be evacuated to an area at least 300 feet away form the threatened area. Greater distances are encourage, if at all possible. In any case, evacuees should be told to take cover and shelter from possible fragmentation.

g. What are the responsibilities of occupants during evacuation? The occupants should open all doors and windows. This will reduce the shock effect of the bomb. Electrical units should be unplugged. This will reduce chance of detonation and reduce noise for an audio check. Then occupants should proceed calmly, following the orders of the evacuation team.

h. Will dog teams be used to search? MP working dogs trained in explosives detection may be used in the search effort. Their acute sense of smell and training allows them to discriminate the scent of explosives, thus, enhancing the search effort.

THIS PAGE INTENTIONALLY LEFT BLANK.

LESSON 3

PRACTICE EXERCISE

REQUIREMENT. The following questions are multiple choice. You are to select one that is correct. Indicate your choice by CIRCLING the letter beside the correct choice directly on the page. This is a self-graded lesson exercise. Do not look up the correct answer from the lesson solution sheet until you have finished. To do so will endanger your ability to learn this material. Also, your final examination score will tend to be lower than if you had not followed this recommendation.

1. When planning a bomb threat search team, the team should never be less than?

A. Two men.
B. Three men.
C. Four men.
D. Eight men.

2. The first sweep of the room search includes which of the following?

A. A quick search first.
B. All objects from the floor to waist level.
C. All objects from the floor to the ceiling.
D. Area built into the walls only.

3. Motives for bomb incidents usually fall into what two categories?

A. Extremists and radicals.
B. Disloyalty and disaffection.
C. Boredom and a lack of interest.
D. Nonpolitical and political.

4. Who WILL NOT be used to search for reported explosive devices?

A. Explosive ordnance personnel.
B. Occupants.
C. Charge of quarters.
D. Building supervisor.

5. Which of the following areas should be activated automatically when a bomb threat is received?

A. Provost marshal operations center.
B. Emergency Operations Center.
C. Command post.
D. Tactical operations center.

6. Who should make critical decisions when dealing with a bomb threat?

A. Provost Marshal.
B. Emergency plans officer.
C. Commander or Bomb Scene Officer.
D. EOC officer.

7. Emergency personnel not involved in searching for a reported explosive should be kept at least how far from the suspected site?

A. 100 feet.
B. 200 feet.
C. 300 feet.
D. 400 feet.

8. Who has the authority to order the evacuation of a building when a bomb threat is received?

A. The commander, supervisor of the building concerned, or bomb scene officer.
B. The senior on-scene officer, regardless of his position.
C. The MPs at the scene of the incident.
D. The post duty officer.

LESSON 3

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

Item		Correct Answer and Feedback
1.	A.	Two men. The smallest search... (page 3-13, para 10b)
2.	B.	All objects from the floor to waist level. The first sweep of... (page 3-15, para 11b(3))
3.	D.	Nonpolitical and political. There are two... (page 3-5, para 4)
4.	A.	Explosive ordnance personnel. Except in the... (page 3-9, para 6b(3)(a))
5.	B.	Emergency Operations Center. Emergency Operations... (page 3-7, para 5e)
6.	C.	Commander or bomb scene officer. The CO or his... (page 3-8, para 6b(1)(a))
7.	C.	300 feet. Occupants should be... (page 3-16, para 13f)
8.	A.	The commander, supervisor of the building concerned... The CO or building... (page 3-16, para 13a)

LESSON 4

EMPLOY INTRUSION DETECTION SYSTEMS

Critical Task: 191-386-0005

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn to determine the necessity and feasibility of an IDS, identify the basic operation, and select the appropriate IDS for the desired security level.

TERMINAL LEARNING OBJECTIVE:

ACTION: Employ intrusion detection system (IDS).

CONDITION: You will have this subcourse, paper and pencil.

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

REFERENCES: The material contained in this lesson was derived from the following publication: FM 19-30 and TM 5-853-4.

INTRODUCTION

Individuals employ security systems as a means of detecting intruders and protecting personal possessions. Likewise, government and industry must have such protection. This will deny access to information, material or equipment which could disrupt the mission or allow the enemy an advantage. Security in depth is the goal of physical security personnel. Such security calls for physical barriers, guards, protective lighting systems and intrusion detection systems. All these provide the protection deemed necessary. Structural barriers are delaying devices. These include gates, fences, locks, and natural barriers. Intrusion detection systems are mechanical and electronic warning systems. They are developed by using basic laws of electricity and are designed to alert security personnel of intrusion or attempted intrusion into an area. These systems are designed, also, to alert security to tampering. This occurs when a person tries to circumvent the intrusion detection system. Certain types of systems are suitable for exterior protection, while others are suitable only for interior use. All have advantages and disadvantages; however, security personnel must remember one main fact: any warning system is valueless unless supported by prompt guard force action and manned by trained operators and monitors. A state of readiness such as this is necessary in the event of alarm activation. A

glossary may be found in Appendix D. This glossary will assist you in understanding IDS.

1. Purpose of IDS. Protective alarm systems are used to accomplish one or more of the following:

a. Economize. IDS permits more economical and efficient use of manpower. It does so by substituting mobile responding guard units for larger numbers of patrols for fixed posts.

b. Substitute. Some IDS are used in lieu of other physical security measures. These are those measures which cannot be used because of safety regulations, operational requirements, appearance, lay-out costs, or other reasons.

c. Supplements. IDS provides additional controls at critical points or areas.

2. Types of Alarm Systems and Specifications. Alarm and communications systems are closely allied in any comprehensive protection system. Telephone and radio communications are common in everyday usage. Because of this, their adaptation to a protective system poses few new problems. An alarm system is simply a manual or automatic means of communicating a warning of potential or present danger. Types of alarm systems include the following:

a. Local Alarm System. A local alarm system is one in which the protected area is directly connected to an alarm bell or siren. The visual or audible signal is located in the immediate vicinity of the object of protection. The light or sounding device must be displayed on the exterior of the building, and it should be fully protected against weather or willful tampering. Also, the device must be audible for a distance of at least 500 feet, if applicable. Response to the alarm is by security guards or other personnel within sight or hearing. They would notify the appropriate security personnel. A residential burglar alarm system is an example of a local alarm system. The major disadvantage is that someone has to hear, see and report the alarm.

b. Direct Connected System. This system is one in which the protected area is directly connected to police or fire departments via a pair of phone wires. These systems insure constant monitoring and quick response to alarms. A major disadvantage is dual responsibility for maintenance, since the user must sell the alarm system to the police in order to install it.

c. Central Station Alarm. In this system a secured area is directly connected to the alarm panel in a centrally located receiving station via phone lines. A commercial agency usually contracts to provide designs and installation. The agency usually provides for maintenance and operation of such systems. They will dispatch guards to the location of the secured area and will also notify police. Alarm installation of this type can only be made when the premises are within 10 minutes of traveling time from the central office. This system is expensive to maintain; however, it insures dedicated

monitoring and response to the alarm. Large jewelry and other commercial stores use this system.

d. Proprietary Alarm System. This system is similar to the central station system except that it is owned by, and located on, the post. The location allows manning at the MP headquarters. The guard force operates and responds to all alarms within the protected area. All alarms are transmitted via phone lines leased from the local telephone company. Advantages include: the system is owned, operated, responded to and maintained by the owner. The guard force, in most cases, has jurisdiction over the intruder. Disadvantages include: expensive initial cost for installation, and lack of skilled personnel for repair and maintenance.

3. Determination of the Necessity and Feasibility. Information presented to this point reveals clear advantages and disadvantages of IDS. As physical security officer, it is your responsibility to provide the most effective physical security measures available. You must do so to provide the depth of security required. Selection of such measures, however, is not based just on personal preference, available resources or type of facility. Consideration must also be given to a number of circumstances.- You must determine the necessity and feasibility of installing an IDS. To make this determination, you must consider the following factors:

a. Mission of the post or facility.

b. Criticality of the post or facility.

c. Vulnerability of the post or facility.

d. Accessibility to intruders.

e. Location of the facility and location of areas to be protected inside the post.

f. Construction of the building.

g. Hours of operation.

h. Availability of other forms of protection.

i. Initial and recurring costs of the system. This should be compared to the cost in money or security or possible loss of materials or information.

j. Design and salvage value of the system.

k. Response time of the security force.

l. Savings in manpower and money over a period of time.

m. Intruder time requirements.

4. Determination of the Degree of Protection. Each type of IDS is designed for a specific type of protection. Therefore, security personnel must analyze and make a determination on the degree of protection. Protection is dependent upon the following factors:

a. The threat. What criminal activity is being deterred, burglary, arson, etc.?

b. The value of assets?

c. Location of the building, room, open area or closed area.

d. Construction of the building or room.

e. Degree of physical security afforded by safes, cabinets, racks, locks, and other supportive security measures.

f. The effectiveness of the intrusion detection system.

g. The responsiveness of the reaction force to the reported intrusion.

5. Desirable Characteristics and Security of Intrusion Detection Systems. Intrusion detection alarm systems should be inherently stable. They should be durable, reliable, and maintainable. These devices are designed to detect, not prevent; they should be used as an adjunct to, not a substitute for, the security force. There are various types of alarm systems. All of them have certain advantages and disadvantages. Desirable characteristics of an alarm system include the following:

a. A detection unit or detection components (normally called sensors). These are located at the protected area. They are designed to initiate an alarm upon intrusion of an intruder into the area. They will alarm, also, upon the approach of a human to a protected object.

b. Signal transmission lines. These lines conduct the alarm signals from the protected area to a central annunciator panelboard. These lines should be constantly monitored.

c. A central annunciator panelboard containing the electronic components. This panelboard announces by both visible and audible signals. It alerts upon intrusion into protected areas and the structure of location involved.

d. Fail-safe features. These give a signal at the annunciator panelboard when abnormal operating conditions keep the alarm system from functioning properly.

e. Other features. These are features which make this system less vulnerable to agents trained to circumvent detection. Such features should include capability of concealment and difficulty of neutralization.

6. Principles of Operation.

a. Intrusion detection devices have had varying degrees of acceptability. This is because they are dependent on effectiveness and reliability. They are also dependent upon cost and maintenance required. No one system is suitable or adaptable to every site and environment. The situations and conditions at the site to be protected determine which devices or systems are efficient and practical.

b. These devices transmit an immediate warning signal, and they operate on the following basic principles:

(1) Breaking of an electric circuit.

(2) Interruption of a light beam.

(3) Detection of sound.

(4) Detection of vibration.

(5) Detection of motion.

(6) Penetration of an electronic field.

(7) Detecting the sudden introduction of a heat source.

7. Classification of Sensors.

a. Intrusion detection sensors are designed for both interior and exterior use. Sensors must be chosen based on intended use. For example, interior sensors are ineffective when exterior perimeter protection is desired.

b. All interior intrusion detection sensors are classified as to what stage of intrusion they are meant to protect. The three classifications are as follows:

(1) Penetration through the perimeter. Initial entry through perimeter barriers is detected. The opening of a window or door to a protected area constitutes perimeter penetration. This can be detected by sensors.

(2) Movement inside the protected area. This type sensor is a motion detector. Energy patterns created by motion detectors change when an intruder moves within a protected area. The sensors automatically detect the changes in energy patterns and respond accordingly.

(3) Point/removal coming in contact with the item being protected. Touching or trying to remove a protected item, such as a vault or safe, triggers the sensor.

8. Electric Circuits.

a. Possible points of entry into buildings or enclosures can be wired. Electrically charged strips of tinfoil or wire are used. An action which breaks the foil or wire interrupts the circuit and activates an alarm. Foil stripping is often used on windowpanes. Doors and windows may be equipped with magnetic or spring activated contacts. These sound an alarm when the door or window is opened. Protective wiring running through concealed wooden dowels may be used on walls and ceilings.

b. Characteristics.

(1) Advantages. These circuits consistently provide the most trouble-free service; they cause few, if any, nuisance alarms. Electric circuits act as a psychological deterrent.

(2) Disadvantages. These circuits are costly to install for many entry points. Their effectiveness may be defeated by the bridging of circuits. Also, this system is not capable of detecting intruders staying behind.

9. Light Beams.

a. This is a photoelectric type of intrusion detection device. It derives its name from the use of a light sensitive cell and a projected light source. An infrared filter over the light source makes the beam invisible to intruders. This device is connected by wires to a control station. When an intruder crosses the beam, he breaks contact with the photoelectric cell. This activates an alarm. A projected beam of invisible light can be effective for approximately 500 feet (see Figure 4-1).

b. Characteristics.

(1) Advantages. When properly used, this device affords effective, reliable notice of intrusion. It may also detect fire through smoke interrupting the light beam.

(2) Disadvantages. Use is limited to those sites where it is not possible to bypass the beam by crawling under or climbing over it. This device requires some type of permanent installation, also. Fog, dust and rain in sufficient density, will interrupt the light beam and produce nuisance alarms. This system requires frequent inspections of light producing components to detect deterioration. Also, the ground beneath the light beam must be kept free of tall grass and weeds, drifting snow and sand.

10. Detection of Sound and Vibration.

a. Detection of Sound.

(1) This type of intrusion detection can be effectively used to safeguard enclosed areas (volmetric), such as vaults, warehouses and similar

enclosures. Passive ultrasonic sound sensor emits no energy but simply "listens" for ultrasonic frequencies produced by breaking through construction materials such as glass, wood, masonry, etc. The sensitivity of this alarm can be adjusted.

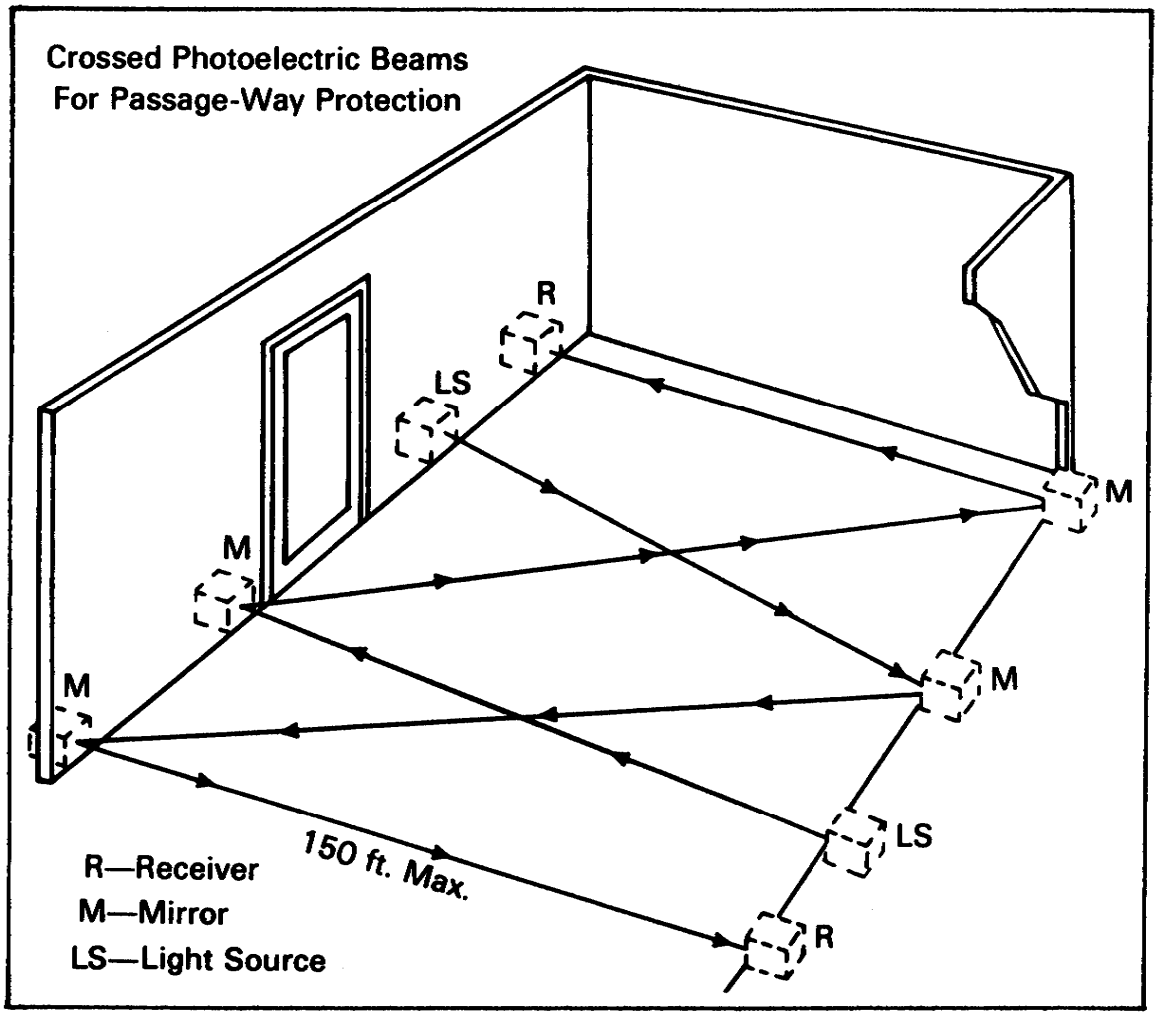


Figure 4-1. Photoelectric IDS.

(2) Characteristics.

(a) Advantages. This device is economical and easily installed. After an alarm is received, the amplifier may be adjusted to monitor sounds coming from the protected area. This system also has high salvage value.

(b) Disadvantages. This device can be used only in vault type installations or other enclosed areas where a minimum of extraneous sound exists. This device is not satisfactory where high ambient noise levels occur, especially traffic. Also, this system cannot be used effectively outdoors. Neither can it be used indoors in areas where sensitive classified discussions occur.

b. Detection of Vibration. This type of detection can operate on one of two principles. The first, known as Piezo Electric, converts energy exerted by the intruder against the structural material into an electrical signal, proportional to the energy exerted, and triggers an alarm. The second is seismic mass, or small weight, and rests on two contacts. When force of impact is applied, the seismic mass is vibrated off of the contacts, breaking the circuit and triggering an alarm. Sensitivity of this alarm cart be adjusted.

(1) Characteristics.

(a) Advantages. Easily installed, economical, flexible in application and salvageable.

(b) Disadvantages. Can only be installed where minimal vibration exists. Heavy construction, railroads, or heavy vehicular traffic creates false alarms. Cannot be used effectively outdoors."

11. Detection of Motion. Motion is detected by ultrasonic sound, microwave (radiowaves), or infrared energy. These types of sensors are volumetric in nature, meaning these sensors are capable of covering a large volume of area.

a. The ultrasonic motion sensor (UMS) operates on a "Doppler Frequency Shift" principle much like police radar. A pattern of inaudible sound waves is transmitted and monitored by the system receiver. Intruders motion within the covered area disturbs the sound wave pattern, altering its frequency or speed. The receiver detects the frequency or "Doppler Shift" and signals an alarm. Caution must be taken not to aim the sensors toward each other unless separated by at least 60 feet. The transmitters/receivers will "talk" or signal each other and they will become ineffective."

(1) Characteristics.

(a) Advantages. This system is easily installed by unskilled personnel and requires minimum installation time. Routine maintenance cost is low. If security interest ends, complete recovery of equipment is possible.

(b) Disadvantages. Sensitivity controls must be carefully adjusted and frequently checked; nuisance alarms may lead security personnel to reduce the system's sensitivity. At low sensitivity, it is sometimes possible to enter a protected area without activating the alarm. This can be done by staying beneath the level of tables or desks; it can also be done by moving so slowly that the ultrasonic waves are not shifted. This system may not be adaptable for use in areas where quantities of absorbent materials are stored, since these absorb sound waves.

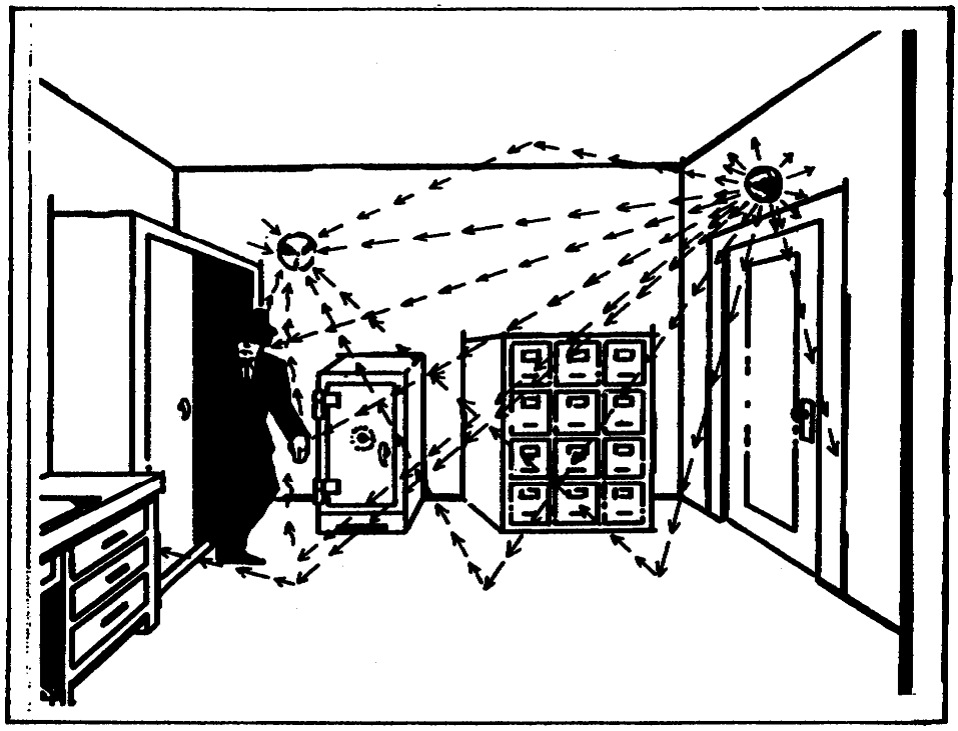


Figure 4-2. Motion Detection Device.

b. Microwave motion detector sends out a carefully controlled amount of microwave energy that is reflected off of walls, floors, ceilings and stationary objects within the area of coverage and returns to the receiver, establishing a pattern. Once the pattern has been established, if any change in that pattern is detected, an alarm is signaled. Unlike the ultrasonic sound, microwave will penetrate wood or glass.

(1) Advantages. Good coverage is provided if antennas are properly located. This system is generally not affected by air current, noise, or sound, and it has high salvage value.

(2) Disadvantages. Coverage is not easily confined to the security area. Fluorescent lightbulbs will activate the sensor.

c. The infrared motion sensor will set up a pattern where it receives infrared energy within a preset zone: an intruder moves from one zone to another; this activates the alarm and causes an increase of infrared energy in one zone and a decrease in the other.

(1) Advantages. This system detects stay behinds. It provides excellent coverage with proper installation, and it has high salvage value.

(2) Disadvantages. Use of this system is limited to the area to be covered, and it is affected by weather change.

12. Capacitance Proximity Sensor. The capacitance or electrostatic intrusion detection system sets up an electrostatic field. This surrounds the object to be protected. This field is tuned by a balance between the electricity capacitance and the electrical inductance. The body capacitance of an intruder who enters the field unbalances the electrostatic energy of the field. This unbalance activates the alarm system.

a. Advantages. This system provides an invisible protective field. It affords a high grade of protection and it is simple to install.

b. Disadvantages. This system can only be applied to metal ungrounded objects; housekeeping of protected area or object must be carefully watched.

13. Weight Director. This is a sensor(s) used to detect the increase of weight, such as a weight mat. It is also used to detect some decrease of weight, such as a scale. This system can be so sophisticated that it can detect weights to .001 of a gram.

a. Advantages. Simple to install, this system is also difficult to defeat. It is easy to hide or camouflage and is salvageable.

b. Disadvantages. The system must be periodically replaced. When cleaning crews are in the area, the system must be deactivated.

14. Closed Circuit Television (CCTV).

a. CCTV is not a true intrusion detection sensor in itself, but it is very useful in physical security operations. Also, it is often used to complement an alarm system. This may be done by placing cameras at critical locations. Doing so will provide direct visual monitoring from a -vantage point. Closed circuit television may be used on gates that are not manned all the time by guards. The system may be used for surveillance of security cages and high value goods in warehouses. Fence lines, movement of cargo, and parking lots may also be watched using this system.

b. CCTV should be enclosed in metal housings which are lockable. This will prevent unauthorized tampering. All cables should be inserted in metal conduit when at all possible.

c. Normal use of TV on gates includes the use of a two-way communication system and an electrically run gate lock. Communication is covered between the monitor panel and the gate. With this device, the guard at the monitor panel can be alerted on the speaker by a person wanting to enter. The guard can determine his authority to enter, and he can then release the gate lock.

d. A great advantage of CCTV is that it can backup IDS sensors. This is helpful when checking out areas before a response force arrives. CCTV also has videotape recording capability.

e. The greatest problem in CCTV usages is the light intensity required for cameras. This requirement must be determined and the availability of

enough light must be verified. Both must be done before the system is bought and installed. Other problems which must be considered are the initial cost of the system; weather conditions may hamper the visibility of the guard especially in making a positive ID and detecting forged or altered ID badges. Another problem to watch for is forceful entry through the gate that was opened for the preceding person.

15. Heat Sensors. Heat sensors can be used to detect smoke or heat. These may be produced by equipment, such as a torch cutting through a vault or other metal walls. Since arson is a great threat to physical security, this sensor can save lives and property.

16. Signal Lines. An alarm system is no better than the security of the lines that transmit the signal. These lines must be sensitive enough to cause an alarm in the event of tampering. An alarm system may be defeated by an intruder. This may happen regardless of how good its triggering mechanism is if the signal line is not functioning right. Lines may be made ineffective. Sometimes an intruder has enough knowledge of electricity and the necessary equipment to adjust the resistance in the line.

17. Communication Systems. Protective communication systems will vary in size and type. Importance, vulnerability, size, location, radio receptivity, and other factors cause the variance. They also affect a specific post and must be largely subject to local determination. Normally, the regular communication system of a post is not adequate for protective security purposes. Guard forces should have their own communication system with direct lines outside. They should also have an auxiliary power supply. Principal dependence is placed on the telephone, teletype, and automatic alarm systems. However, interior and exterior radio communications play a large part, also, in the protection of large posts. One or more of the following means of communication should be included in this system:

a. Facilities for local exchange and commercial telephone service.

b. Intraplant, interplant, and interoffice telephone systems. These should utilize either government owned or rented circuits and equipment, but they should not be interconnected with facilities for commerce or toll telephone service.

c. Radiotelephone and/or radiotelegraph facilities for either point to point or mobile service.

d. Telegraph and teletype facilities for either commercial or private operation.

e. Central station automatic alarm system.

f. Hand-carried portable radios and/or receivers. These should have transmitters stationed strategically throughout the post.

g. Guard supervisory system having key operated electric call boxes. These should be located strategically throughout the post. By inserting the key in a cell box, a guard can make a routine tour report or summon emergency aid. Tampering with the transmitting key or the call box automatically locks the box. This causes a failure of the signal and an alert for immediate investigation.

18. Alternate Communication System. Alternate communication systems are always advisable for use in emergencies. A flood of inquiries follows emergency conditions. Added to the normal flow of messages, the calls may overload the existing system at the very time that sure and rapid communication is vital. The most efficient emergency reporting system consists of direct connection to the guard or communications center from telephones strategically placed throughout the post. Use of these telephones should be restricted to emergencies and guard reporting only. Wires of alternate systems should be separated from other communication lines, and they should be in underground conduits. For emergency communication with agencies off post, leased wires or a radio adjustable to civil police and fire department frequencies should be available.

19. Joint Services Interior Intrusion Detection System (J-SIIDS). J-SIIDS was designed for standardized use by the DOD. The J-SIIDS has a high detection capability with low nuisance alarms when properly installed and proper phone lines are used. In this text, nuisance alarms are those whose activation results from other than the actions of a perpetrator. For example, stray animals, wind, dust, tall grass, etc., may activate alarms.

a. Use of J-SIIDS. The system was mainly designed for use and security of arms, ammunition, and explosives (AA&E) areas; however, it had been certified for use in finance offices, PXs, aircraft hangars, and narcotics storage areas. All commercial systems used in lieu of J-SIIDS will be tested and technically reviewed in accordance with AR 190-13 before purchase and installation.

b. This system consists of a family of sensors that can be used singly or in combination. It is to provide detection of intrusion. Sensors are grouped into the following four categories:

(1) Penetration.

(2) Point.

(3) Motion.

(4) Duress.

c. Under current regulation, AA&E protected by an IDS will use at least two types of sensors (i.e., penetration and motion).

THIS PAGE IS LEFT BLANK INTENTIONALLY

LESSON 4

PRACTICE EXERCISE

REQUIREMENT. The following questions are multiple choice. You are to select the one that is correct. Indicate your choice by CIRCLING the letter beside the correct choice directly on the page. This is a self-graded lesson exercise. Do not look up the correct answer from the lesson solution sheet until you have finished. To do so will endanger your ability to learn this material. Also, your final examination score will tend to be lower than if you hand not followed this recommendation.

1. When an alarm system protecting an area is directly connected to an alarm bell or siren, it is what type alarm system?

A. Central.
B. Local.
C. Direct.
D. Proprietary.

2. Intrusion detection sensors are classified according to which of the following?

A. Exterior and/or interior use.
B. Protection at various stages of intrusion.
C. Sensitivity of sound and vibration.
D. Ability to identify changes in energy patterns.

3. Of the following which is NOT a disadvantage of interrupting a light beam?

A. Garbage.
B. Smoke interruption.
C. Boxes in aisle.
D. Loose animals.

4. Commercial systems, used in lieu of J-SIIDS, designs and installation must be approved in accordance with?

A. AR 190-13.
B. FM 19-30.
C. AR 190-14.
D. AR 190-16.

5. J-SIIDS is NOT certified for use in which of the following storage areas?

A. Narcotics.
B. Arms, ammunition and explosives.
C. Nuclear fuel.
D. Post exchange.

6. Which of the following is NOT one of the three classifications of sensors?

A. Penetration.
B. Direct.
C. Motion.
D. Point.

LESSON 4

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

Item		Correct Answer and Feedback
1.	B.	Local A local alarm... (page 4-2, para 2a)
2.	B.	Protection at various stages of intrusion All interior... (page 4-5, para 7b)
3.	B.	Smoke interruption It may also... (page 4-6, para 9b(1))
4.	A.	AR 190-13 All commercial... (page 4-12, para 19a)
5.	C.	Nuclear fuel The system was... (page 4-12, para 19a)
6.	B.	Direct The three... (page 4-5, para 7b)

APPENDIX A

BOMB THREAT DATA

FBI BOMB DATA CENTER

PLACE THIS CARD UNDER YOUR TELEPHONE

QUESTIONS TO ASK:

1. When is bomb going to explode?
2. Where is it right now?
3. What does it look like?
4. What kind of bomb is it?
5. What will cause it to explode?
6. Did you place the bomb?
7. Why?
8. What is your address?
9. What is your name?

EXACT WORDING OF THE THREAT:

_____

_____

_____

_____

_____

_____

_____

_____

_____

Sex of caller: _____ **Race:** _____

Age: _____ **Length of call:** _____

Number at which call is received:

_____

Time: _____ **Date:** __/__/__ FBI/DOJ

BOMB THREAT

CALLER'S VOICE:

____ Calm	____ Nasal
____ Angry	____ Stutter
____ Excited	____ Lisp
____ Slow	____ Raspy
____ Rapid	____ Deep
____ Soft	____ Ragged
____ Loud	____ Clearing throat
____ Laughter	____ Deep breathing
____ Crying	____ Cracking voice
____ Normal	____ Disguised
____ Distinct	____ Accent
____ Slurred	____ Familiar
____ Whispered	

If voice is familiar, who did it sound like?

_____

_____

BACKGROUND SOUNDS:

____ Street noises	____ Factory machinery
____ Crockery	____ Animal noises
____ Voices	____ Clear
____ PA System	____ Static
____ Music	____ Local
____ House noises	____ Long distance
____ Motor	____ Booth
____ Office machinery	Other _____
	_____
	_____

THREAT LANGUAGE:

____ Well spoken (educated)	____ Incoherent
____ Foul	____ Taped
____ Irrational	____ Message read by threat maker

REMARKS: _____

_____

_____

_____

Report call immediately to:

_____ .

Phone number _____ .

Date __/__/__ .

Name _____ .

Position _____ .

Phone number _____ .

APPENDIX B

AFTER ACTION REPORT

ATZN-XXX-XX (Office Symbol Bomb Scene Officer) 30 May 19XX

MEMORANDUM FOR POST COMMANDER

SUBJECT: Bomb Threat Incident/Accident Report

PART I: Bomb Threat

1. NATURE OF INCIDENT.

a. Who received call?

b. Where was call received?

c. Telephone number of line to which call was made.

d. Date and time of call.

e. What caller said and the response of receive, if any.

f. Was caller male or female? Approximate age of caller.

g. Any unusual speech characteristics of the caller, such as accent.

2. ACTION TAKEN.

a. Who was notified immediately after call was received?

b. Time of evacuation, if applicable.

c. Search techniques employed.

d. What was discovered, if anything?

e. If there was an evacuation, at what time did personnel reenter the building?

PART II. INCIDENT OF BOMB DISCOVERY

1. NATURE OF INCIDENT.

a. How was bomb discovered?

ATZN-XXX-XX (Office Symbol of Bomb Scene Officer)
SUBJECT: Bomb Threat Incident/Accident Report

a. Place of discovery.

b. Who discovered it?

c. Date and time of discovery.

d. Was it established that only one bomb existed?

e. Description of the device.

PART III: INCIDENT OF BOMB DETONATION

1. NATURE OF INCIDENT.

a. Where bomb exploded.

b. Date and approximate time of explosion.

c. Who reported incident.

2. ACTION TAKEN.

a. What members of the search and EOD teams arrived on the scene?

b. About what time?

c. How were the injured, if any, treated/evacuated?

3. OUTCOME.

a. Extent of property damage, if known.

b. Was building secured for further investigation?

c. Number of persons killed or injured.

4. ADDITIONAL INFORMATION.

Give color and description of sound of explosion, if observed.

HAROLD J. HENRY
LTC, MP
Bomb Scene Officer

APPENDIX C

SEARCH CHECKLIST

YES	NO	
__	__	Were all areas assigned to some member of the search team?
__	__	Was the outside of the building and surrounding area searched?
__	__	Were the assignments to areas based on knowledge of the area?
__	__	Was key control established; were all doors unlocked?
__	__	Did search team members know their area assignments?
__	__	Did search team members know their responsibilities when a bomb or suspected bomb was found?
__	__	Were communication procedures established?
__	__	Were proper search techniques followed?
__	__	Was there an audio check?
__	__	Were rooms divided by area?
__	__	Were rooms divided by height?

What actions were taken when a "bomb" was found? _____

_____

What search techniques were used? _____

_____

What method(s) of communication was used? _____

_____

What areas were not searched? _____

_____

APPENDIX D

GLOSSARY

Actuator	A holdup button, magnetic switch or thermostat that will cause the system to alarm.
Alarm System	Combinations of compatible intrusion detection devices, arranged to support one another.
Ambient	Sound, encompassing the surrounding atmosphere.
Annunciator (Monitor)	A visual or audible signalling device that indicates conditions of associated circuits. Usually, this is done by the dropping of a shutter or by activating a signal lamp and by audible sound.
Antenna	A conductor or system of conductors for radiating or receiving electromagnetic waves.
Capacitance	The property of two or more bodies which enables them to store electrical energy in an electrostatic field between them; it is measured in farads.
Control Unit	A facility, consisting of switches, potentiometer, and audible and visible alarms. Also included are the system "on-off" switch, and possibly an annunciator system where more than one circuit is monitored; this unit is usually installed at a point manned full time by a guard.
Data Transmission System	Component consisting of data transmitter in the control unit and a data receiver in the monitor unit; it is the communication link used to pass alarm and equipment status signals from the control unit to the monitor unit. This is done over a wire transmission line or by radio frequency.
Fail Safe	A term applied to a device or system so designed that, in the event of a failure of some component to function properly, the device will, by a signal or otherwise, indicate its incapacity.
False Alarm	Activation of sensor(s) for which no cause can be determined.
Intrusion Detection System	The combination of components, including sensors, control units, transmission lines, and monitor units integrated to operate in a specified manner.

Joint Service Interior Intrusion Detection System (J-SIIDS)	Developed as a standard detection system for joint-service application; for protection of military arms rooms and other inside areas.
Monitor	A device that senses and reports on the condition of a system; commonly used interchangeably with the terms monitor unit, monitor panel(s), annunciator, and other similar terms.
Overload	A load greater than the rated load of an electrical device.
Receiver	An electromechanical device for detecting and converting electromagnetic energy into sound waves.
Signal Lines	Cable pairs or wire lines through which signal or electrical currents are transmitted from one station to another.
Sonic	Of, pertaining to, or designating the speed of sound in air; i.e., about 1087 feet per second at 32 degrees fahrenheit or about 740 miles per hour.
Transmitter	The apparatus for converting sound waves into electrical waves.
Transducer	A device that transfers or changes one type of energy into another form. An example is a loud-speaker which changes electrical into acoustical (mechanical) energy.
Underload	Less than a normal amount of current flowing through an electrical device.

★U.S. GOVERNMENT PRINTING OFFICE:1999-728-075/01053