Student Guide

Course: Physical Security Measures

Lesson 1: Course Introduction

Course Information

Purpose	Provide a thorough understanding of the types of physical security measures available to protect DoD assets as well as the uses for and purpose of each type of physical security measure
Audience	Military, civilian, and contractor personnel responsible for physical security
Pass/Fail %	75% on final examination
Estimated completion time	120 minutes

Course Overview

Physical security measures are security measures employed to prevent or reduce the potential for sabotage, theft, trespassing, terrorism, espionage, or other criminal activity. To ensure security, the security measures must provide the capability to deter, detect, identify, track, assess, record, communicate, delay, and respond to unauthorized access activities.

Security operations and procedures must ensure the effective protection of Department of Defense (DoD) assets. Security requirements for classified contracts are stated in DoD 5220.22M, the National Industrial Security Program Operating Manual (NISPOM.) Any additional security requirements levied upon a contractor must be specifically addressed in the contract.

This course is about the application of active and passive complementary physical security measures, also known as security-in-depth, to protect DoD assets from potential threats.

Course Objectives

At the end of this course, you will be able to—

- Identify key concepts related to security-in-depth
- Identify the various types of physical security measures and their uses

Course Structure

- Course Introduction
- Security-in-Depth
- Exterior Physical Security Measures
- Security Forces
- Security Technology and Equipment
- Course Conclusion

Student Guide

Course: Physical Security Measures

Lesson 2: Security-In-Depth

Lesson Introduction

Before you learn about the various physical security measures and their purposes, there are some concepts related to physical security you should know. This lesson will familiarize you with these concepts.

The lesson objectives are:

- Define security-in-depth
- Distinguish between point security and area security
- Define enclaving

Security-in-Depth

1. Overview

Security-in-Depth is a determination by the senior agency official that a facility's security program consists of layered and complementary security controls sufficient to deter, detect, and document unauthorized entry and movement within the facility. This is accomplished through the integration of active and passive complementary physical security measures.

Think of security-in-depth as integrating layers of security to protect DoD assets. By layering protection through facility planning, the use of barriers, fencing, signs, site lighting, and advanced technologies such as intrusion detection systems, closed circuit television (CCTV) and biometric entry control systems, critical assets can be well protected against a multitude of potential threats. Security-in-depth employs various security measures in levels because different assets require different levels of protection.

2. Concepts

Achieving security-in-depth is the goal of the individuals who are responsible for the security of an installation or activity. To achieve this goal, you must determine the capabilities available and the requirements and needs for security protection such as point versus area security. Both are used to protect DoD assets from damage, loss, and

theft. For example, a small arms storage locker would not be afforded the same degree of protection as an ammunition depot.

When an individual resource requires individual protection, you would employ point security to provide that protection. To protect consolidated resources, such as an installation or facility, you would use area security to provide the best protection.

As a security professional, you should employ both point and area security to protect DoD assets from damage, loss, and theft. In some cases, security-in-depth can be obtained by designating islands of extreme or high security within a sea of moderate security. This is known as enclaving.

Review Activity

Match each term to its definition. Check your answers in the Answer Key at the end of this Student Guide.

A. Point Security B. Enclaving C. Area Security D. Security-In-Depth	___	Integrating layers of security to protect DoD assets
	___	Guarding a specific asset or resource
	___	Protecting an entire area such as an installation or facility
	___	Designating islands of high security within a sea of moderate security

Lesson Conclusion

In this lesson you learned about key concepts related to physical security, such as security-in-depth, point security, area security, and enclaving.

Answer Key

A. Point Security
B. Enclaving
C. Area Security
D. Security-In-Depth

D	Integrating layers of security to protect DoD assets
A	Guarding a specific asset or resource
C	Protecting an entire area such as an installation or facility
B	Designating islands of high security within a sea of moderate security

Student Guide

Course: Physical Security Measures

Lesson 3: Exterior Physical Security Measures

Lesson Introduction

As you learned previously, security-in-depth occurs when layers of security are used together to increase the amount of protection provided a DoD asset. This lesson will help you understand the components used in the outer layers of security-in-depth. These exterior physical security measures help to deter or delay unauthorized entry into DoD facilities, installations, and other protected areas.

The lesson objectives are:

- Identify the types of protective barriers and the purpose and uses for each type
- Identify the types of site lighting and the purpose and uses for each type

Protective Barriers

1. Overview

The first line of defense in any physical security system is usually some form of perimeter protection system. The perimeter of an installation or facility is the outermost area of responsibility. Signs, barriers, and fences are integral parts of this protection.

They are used to establish legal boundaries, to deter individuals from attempting unlawful or unauthorized entry, and to prevent outsiders from being able to view what may be occurring inside the perimeter. Barriers can also be used to direct traffic flow and can serve as platforms for sensors and lighting.

2. Signage

Signage serves many purposes on DoD installations and facilities. Signs can be informational to communicate messages, such as directing individuals to various locations, or they can be regulatory and serve as a deterrent, such as establishing boundaries for restricted areas. Signs may be used to identify physical security boundaries, prohibited and unauthorized material, controlled or sensitive areas, an area under surveillance, or security force personnel and vehicles. For some types of signs, specific wording or the sign's content, color, and size are mandated by regulation. Signs for other purposes may be locally designed.

Some factors to consider for effective use of signs are the language on the sign, what material is used to make the sign, whether the sign is reflective or non-reflective, placement of the sign, how the sign is mounted, whether the sign is lit or unlit, and what maintenance will be required for the sign.

3. Fencing

Fencing can be either permanent or temporary.

Permanent fencing is used when a stationary perimeter requires protection. Materials used are dictated by the degree of protection required. For example, a perimeter may be defined with a chain link fence. While economical, a chain link fence may not afford the amount of protection as one equipped with barbed or concertina wire, or reinforced with steel cables.

Temporary fencing can be used as a temporary perimeter to establish psychological barriers and to channel pedestrian and vehicle movement. Several temporary fencing materials are available, including plastic netting, rolled wooden slats or support wire fencing, and fixed panels of chain link fencing. Additionally, both barbed wire and concertina wire can be used as temporary as well as permanent fencing.

a. Chain Link Fencing

Chain link is one of the most common types of permanent fencing material. It is used primarily to define a perimeter, and it may not be the most secure means to protect an asset. Chain link fences are not resistant to a determined intruder, who could climb over the fence or use wire or bolt cutters to breach the fence. Also, chain link fencing does not afford protection against visual observation, although plastic or wooden inserts can be used to achieve a degree of privacy. Component-defined specifications may include minimum height, gauge or thickness of wire, mesh opening size, twisted and barbed ends, method of fastening to posts, ground requirements, method of installing posts, fence fabric reinforcement, paint color requirements, top guard dimensions and materials, and gate considerations.

b. Barbed Wire

Barbed wire can be used as permanent fencing or as a temporary barrier. An entire fence can be made of barbed wire with posts and used as either a permanent or temporary barrier. Barbed wire can also be used as a permanent barrier when it is installed as an outrigger or top guard on top of a chain link fence. When barbed wire outriggers are used, they may be slanted outward, inward, or both, depending on the nature of the asset being protected. Barbed wire can be used as a temporary barrier simply by uncoiling it and laying it on the

ground, which is most common in a tactical environment. Component-defined specifications may include overall fence height, wire size, number of barbs, post spacing, distance between strands, and interlacing requirements.

c. Concertina Wire

Concertina wire, also known as razor wire, is a commercially manufactured wire coil of high-strength steel barbed wire, clipped together at intervals to form a cylinder. It is widely used to warehouses, prisons, military installations, and field locations. Concertina wire can be used as permanent fencing when used as an outrigger on top of a chain link fence. This is a common use in combat environments to prevent unauthorized entry into an area or installation. It can also be used as a temporary barrier by simply uncoiling the wire and laying it on the ground to create an obstruction. This use of concertina wire typically occurs in a tactical environment or as a temporary barrier until a permanent one can be erected. Multiple layers of concertina wire create an even more secure perimeter, by using two parallel rows with a third row in a pyramid configuration. While concertina wire is secure and age resistant, it can be difficult to handle and may hamper ground maintenance. Component-defined specifications for using concertina wire may apply.

d. Plastic Netting

Plastic netting is commonly used as a temporary barrier around construction sites and may also be used for crowd control. The netting is a good resource for clearly identifying areas personnel should not enter. The fencing material is not very sturdy and is easily defeated. Its primary role is to prevent accidental entry into a given area, and it should not be relied upon for protection of essential resources.

e. Rolled Wooden Slat Fencing

Rolled wooden slat fencing provides a temporary security barrier and also prevents observation from outside the protected area. The fencing can be used in a number of different situations but should not be relied upon as the sole security measure to protect essential resources.

f. Fixed Panel Chain Link Fencing

Fixed panel chain link fencing is commonly used to provide perimeter security, crowd control, and identification of area boundaries. This moderate-security fencing may also be used during construction projects and is often equipped with a locking gate, further preventing unauthorized access. The fence panels are generally stable, durable, and relatively easy to install. They may be equipped

with concrete block foundations or heavy metal footings to prevent them from falling over.

4. Barriers

After the terrorist attacks on September 11, 2001, you may have noticed more barriers appearing in front of federal buildings and DoD installations and facilities. These barriers may have taken up some parking spaces or forced you to walk a longer distance to or from a building. However, as you can now see they were put in place for a reason, to protect U.S. personnel and assets from potential terror attacks. Barriers can be used to channel traffic through designated access control points where pedestrians, vessels, and vehicles can be monitored and searched for contraband, explosives, or other types of unauthorized or prohibited items. Barriers may be composed of several types of material. We will discuss these in broad categories of active barriers, passive or fixed barriers, and natural barriers.

a. Active Barriers

Barrier systems are considered active if they require action by personnel or equipment to permit entry. Active barrier systems define the perimeter and ensure only authorized personnel are permitted access.

Some examples of active barrier systems are gates manually operated by security forces, hydraulic pop-up vehicle barriers, and electronically operated gates or turnstiles.

b. Passive Barriers

Barrier systems are considered passive if their effectiveness relies on their bulk or mass and they have no moving parts. Barrier systems are considered fixed if they are permanently installed or if heavy equipment is required to move or dismantle the barriers.

Some examples of passive and fixed barriers are perimeter or vehicle barriers, temporary barriers, building perimeter barriers, and interior barriers. Perimeter protection systems can include manmade obstacles such as barricades and vehicle barriers to provide for difficult approaches or exit routes. Temporary walls and rigid barriers can be employed to establish barriers against high-speed vehicle approaches to DoD installations and facilities. These structures can be installed along approaches within an installation's boundary to force vehicles to make tight, slow turns before approaching gates or building entrances. These kinds of barriers include concrete vehicle barriers, called Jersey barriers, concrete or sand-filled oil drums, concrete bollards or planters, and earthen excavations such as trenches or berms.

Perimeter barriers that surround buildings vary from those with industrial-type perimeter fences to those composed of little more than attractive landscaping. Considerations in building perimeter barriers include exterior doors, windows, and utility access.

Barriers may be used inside facilities to accomplish the same functions as an installation's access barriers. Interior barriers establish boundaries or lines of demarcation of different activities and differing levels of security within a facility. They may deter individuals from attempting unauthorized entry. They may also be platforms on which intrusion detection systems can be mounted. Barriers may be used within a facility to channel pedestrian and service vehicle traffic.

c. Natural Barriers

Natural barriers can assist in defining boundaries, and may provide adequate perimeter protection in some situations. Examples of natural barriers include waterways, forestations, mountains, deserts, and ditches.

5. Clear Zones

A clear zone is an area inside and outside the perimeter fence or barrier of the protected area. Clear zones provide increased effectiveness of physical barriers, allow security forces to have unimpeded observation, and prevent intruders from being able to hide.

To be effective, clear zones should be free of all obstacles, topographical features, and vegetation.

Site Lighting

1. Overview

Site lighting is used for several purposes in support of physical security. Site lighting supplements other protective measures such as patrols, barriers, and alarms by

illuminating approaches to an area, offering surveillance capability, deterring unauthorized entry, and enabling guard forces to observe activities inside or around an installation or facility and enabling them to conduct inspections of personnel and vehicles.

Good protective lighting is achieved by adequate, even light upon bordering areas, glaring light in the eyes of an intruder, and relatively little light on security personnel and patrol routes. In addition to seeing long distances, security forces must be able to see low contrasts, such as indistinct outlines or silhouettes, and must be able to spot an

intruder who may be exposed to view for only a few seconds. Higher levels of brightness improve all of these abilities.

2. Planning and Implementation

In planning site lighting, there are various factors to consider such as contrast between intruder and background, surfaces to be illuminated, placement of controls and switches, power sources, wiring, and maintenance.

High-brightness contrast between intruder and background should be the first consideration. The volume and intensity of lighting varies with the surfaces to be illuminated. Dark, dirty surfaces, or surfaces painted with camouflage require more illumination than installations and buildings with clean concrete, light brick, or glass surfaces. Rough, uneven terrain with dense underbrush requires more illumination to achieve a constant level of brightness than do manicured lawns.

In planning for placement of controls and switches for protective lighting systems, keep in mind that they should be inside the protected area and locked or guarded. Or, as an alternative, locate controls in a central station similar to, or as a part of, the system used in intrusion-detection alarm central monitoring stations.

The power source for security lighting is normally a public utility company. Site lighting should have an alternate or emergency source of power such as standby batteries or generators and they should be located within a controlled area for additional security.

The system should be tested under load frequently. Wiring systems for site lighting should be implemented and managed to minimize sabotage and vandalism. Protective lighting is inexpensive to maintain, and when properly deployed, may reduce the need for additional security forces. Areas to consider for maintenance include bulb replacement and environmental conditions.

3. Types

There are four types of site lighting used by DoD installations and facilities. They are continuous, standby, emergency, and movable.

a. Continuous Site Lighting

Continuous site lighting is the most common security lighting system. Continuous lighting consists of a series of fixed lights arranged to flood an area continuously with overlapping cones of light during hours of darkness. The advantage of using overlapping cones of light is if a single lamp fails, the area will still remain lit. There are three methods of continuous lighting, which are glare projection, controlled lighting, and surface lighting.

Glare projection uses lights slightly inside a security perimeter and directed outward. The glare projection lighting method is considered a deterrent to potential intruders because it makes it difficult to see the inside of the area being protected. It is useful when the glare of lights directed across surrounding territory neither annoys nor interferes with adjacent operations. Glare projection lighting also protects guard forces by keeping the guards in comparative darkness and enabling them to observe intruders at a considerable distance beyond the perimeter.

Controlled lighting is best used when it is necessary to limit the width of the lighted strip outside the perimeter of a facility or installation so it will not interfere with adjoining properties, nearby highways, railroads, navigable waters, or airports. The width of the lighted strip can be controlled and adjusted to fit the particular need such as illumination of a wide strip inside a fence and a narrow strip outside, or flood lighting a wall or roof. Unfortunately, this method of lighting often illuminates or silhouettes security personnel as they patrol their routes.

Surface lighting is used to light the surface of a building to display a silhouette of any person passing between the light source and the building or show the contrast of a person inside the building.

b. Standby Site Lighting

Standby lighting is similar to continuous lighting except the lamps are not continuously lit. They are used when additional lighting is necessary and may be activated by an alarm or motion detector.

Standby lighting can be very effective in deterring intruders by drawing attention to an area where an intruder has activated the light.

Lamps with a short strike/restrike time should be used for standby lighting as they employ lights immediately when needed. In addition to significant deterrent value, standby lighting also offers economical value in power consumption savings.

c. Emergency Site Lighting

Emergency lighting is used during a power failure or when regular lighting is not available for any reason. This type of lighting depends on alternative power sources such as batteries or generators.

d. Movable Site Lighting

Movable lighting consists of manually operated, movable towers or searchlights that may be lit during hours of darkness or only as needed. Movable light systems are typically used to supplement continuous or standby lighting and can be either portable or stationary.

Job Aid

Take a moment to review this chart, which summarizes the characteristics of various types of lights used in physical security:

LIGHT SOURCE COMPARISON CHART

CHARACTERISTICS	INCANDESCENT	FLUORESCENT	MERCURY VAPOR	METAL HALIDE	HIGH PRESSURE SODIUM	LOW PRESSURE SODIUM
WATTAGES (LAMP ONLY)	UP TO 3,000	40 TO 215	40 TO 1,000	50 TO 1,000	35 TO 1,000	35 TO 180
LIFE (HOURS)	750 TO 2,000	12,000 TO 20,000	16,000 TO 24,000	6,000 TO 20,000	16,000 TO 24,000	18,000 TO 20,000
LUMENS PER WATT (LAMP ONLY)	10 TO 38	67 TO 83	45 TO 63	80 TO 100	80 TO 140	130 TO 183
COLOR RENDITION	EXCELLENT	GOOD TO EXCELLENT	FAIR TO GOOD	EXCELLENT	FAIR TO GOOD	POOR
LIGHT DIRECTION CONTROL	GOOD TO EXCELLENT	FAIR	GOOD	GOOD	GOOD TO EXCELLENT	FAIR
SOURCE SIZE	COMPACT	EXTENDED	COMPACT	COMPACT	COMPACT	EXTENDED
COMPARATIVE FIXTURE COST	LOW	MODERATE	THE REST ARE HIGHER THAN INCANDESCENT AND GENERALLY HIGHER THAN FLOURESCENT			
WARM-UP TIME	INSTANT	INSTANT	5 TO 8 MIN.	5 TO 8 MIN.	2 TO 5 MIN.	5 TO 8 MIN.
RESTRIKE TIME	INSTANT	INSTANT	10 TO 20 MIN.	10 TO 20 MIN.	1 MIN.	0 TO 8 MIN.

Review Activity

Try answering the following questions. When you are finished, see the Answer Key at the end of this Student Guide to check your answers.

Activity 1

Select True or False for each statement. Check your answers in the Answer Key at the end of this Student Guide.

	True	False
Barbed wire and concertina wire may serve as a protective barrier by simply uncoiling it and laying it on the ground.	○	○
Barbed wire is also known as razor wire.	○	○
Jersey barriers may be placed around buildings to prevent vehicles from getting too close to the buildings.	○	○
Rapidly flowing rivers are considered active barriers.	○	○

Activity 2

Which of the following protective barriers would most likely be utilized for its decorative appeal? Select the best answer.

- ○ Trench
- ○ Berm
- ○ Concrete planter
- ○ Jersey barrier

Activity 3

To be effective, clear zones should be free of which of the following? Select the best answer.

- ○ Trimmed grass
- ○ Bushes
- ○ Dirt
- ○ Fencing

Activity 4

Match each characteristic to the lighting-related term to which it applies. Check your answers in the Answer Key at the end of this Student Guide.

Characteristics	Type of Continuous Site Lighting
A. This method is intended to display a silhouette of any person passing between the light source and the building or to show the contrast of a person inside the building.	___ Glare Projection
B. This method is intended to make the inside of a protected area difficult to see from outside the protected area.	___ Controlled Lighting
C. This method is intended to limit the width of the lighted strip outside the perimeter of a protected area so as not to interfere with adjoining property, nearby highways, railroads, navigable waters, or airports.	___ Surface Lighting

Activity 5

Select True or False for each statement. Check your answers in the Answer Key at the end of this Student Guide.

	True	False
When planning protective site lighting, you should ensure that controls and switches are installed inside the protected area and locked or guarded or inside a central station such as an alarm monitoring station.	○	○
Flashlights are a reliable form of continuous lighting.	○	○
Emergency lighting depends upon the power supply of the utility company.	○	○
Standby lighting is the type of lighting used when the primary power source fails.	○	○

Lesson Conclusion

In this lesson you learned about protective barriers and site lighting, which are both used as exterior physical security measures by the DoD.

Answer Key

Activity 1

	True	False
Barbed wire and concertina wire may serve as a protective barrier by simply uncoiling it and laying it on the ground.	●	○
Barbed wire is also known as razor wire.	○	●
Jersey barriers may be placed around buildings to prevent vehicles from getting too close to the buildings.	●	○
Rapidly flowing rivers are considered active barriers.	○	●

Activity 2

Although decorative, a concrete planter can serve as a protective barrier by preventing vehicle access.

Activity 3

A clear zone is an area inside and outside the perimeter fence or barrier of the protected area. An effective clear zone must be free of visual obstructions such as bushes.

Activity 4

Characteristics	Type of Continuous Site Lighting
A. This method is intended to display a silhouette of any person passing between the light source and the building or to show the contrast of a person inside the building.	_B_ Glare Projection
B. This method is intended to make the inside of a protected area difficult to see from outside the protected area.	_C_ Controlled Lighting
C. This method is intended to limit the width of the lighted strip outside the perimeter of a protected area so as not to interfere with adjoining property, nearby highways, railroads, navigable waters, or airports.	_A_ Surface Lighting

Activity 5

	True	False
When planning protective site lighting, you should ensure that controls and switches are installed inside the protected area and locked or guarded or inside a central station such as an alarm monitoring station.	●	○
Flashlights are a reliable form of continuous lighting.	○	●
Emergency lighting depends upon the power supply of the utility company.	○	●
Standby lighting is the type of lighting used when the primary power source fails.	○	●

Student Guide

Course: Physical Security Measures

Lesson 4: Security Forces

Lesson Introduction

An important component of physical security protection for our DoD assets is our security forces. These security forces are composed of DoD personnel, contractor personnel, and even trained dogs. They all have the same mission—to protect DoD assets.

The lesson objective is:

- Identify the types of security forces and the purposes of each type

Use of Security Forces

1. Overview

The majority of DoD installations and facilities maintain a specially identified group of personnel who serve as the enforcement medium for the physical security program. Typically, the security force is deployed to support either point or area security.

Whether government, military or civilian, or contract forces are involved, there is a need to define the criticality of the asset being protected and the jurisdictional authority.

Defining these factors in turn will define the use of force. For example, is use of non-lethal weapons appropriate? Or would use of deadly force be appropriate and authorized?

Once trained and deployed, security forces may require mandatory refresher training to maintain a level of proficiency.

2. Deployment

Security forces are deployed in various ways. Here are some examples of how they are deployed.

Static observation posts, which guard a high priority resource, are used when continuous surveillance is required. Access control points that monitor entry to a facility or secure area may be manned continuously or on a part-time basis. Roving patrols ensure the

safety and security of the installation or facility including personnel, information, equipment, and other DoD assets. Roving patrols can cover large areas in a timely manner. Response forces respond to alarms and incidents. Security system monitors observe alarms and closed circuit televisions. Dispatch control centers dispatch response forces and mobile patrols, and coordinate activities with other personnel. This function may be combined with the security system monitor function.

3. Government Security Forces

Government security forces are made of up government employees who are either military personnel or civilians. Military personnel may either have a full-time job specialty of security or security may be assigned as an additional duty. Civilian physical security personnel are considered part of the security force team and may fill positions in any of the following job series: Security Administration Series, Security Clerical and Assistance Series, Guard Series, Police Series, General Investigating Series, or Criminal Investigating Series.

Whether military, civilian, or government contracted, security forces have the same mission, which is to protect DoD assets.

4. Contract Security Forces

Contract security forces are comprised of non-DoD personnel who are employees of private or commercial sources contracted by the federal government.

Government representatives perform administrative oversight of contract security forces. This oversight may include preparation of standard operating procedures, or SOPs, instructions, or post orders. These all serve the purpose of communicating the government's requirements to the contractor, so great care must be taken in developing these documents.

Security personnel sometimes play a role in defining specifications for guard force contracts. This information is used by contractors to provide cost estimates.

Remember, whether government or contract, all security forces have the same mission—to protect DoD assets.

5. Military Working Dogs

Military working dogs (MWD), also known as K-9s, are an integral part of the physical security program. Military working dogs enable security force members to enforce laws and regulations, suppress the use of illegal drugs, detect explosives, and protect DoD installations, facilities, and resources.

These dogs can also deter attack and defend their handlers during threatening situations. Military working dogs may assist in confrontation management, to search for subjects both indoors and outdoors, and to guard subjects once they are captured. All of these duties are performed during law enforcement activities as directed by their handlers.

Man's best friend is one of our nation's most valuable assets in our physical security mission of protecting DoD assets.

Review Activity

Try answering the following questions. When you are finished, see the Answer Key at the end of this Student Guide to check your answers.

Activity 1

Select True or False for each statement. Check your answers in the Answer Key at the end of this Student Guide.

	True	False
Government security forces may be either military or civilian.	○	○
Contract security forces may be either military or civilian.	○	○
Military working dogs can seek, detect, defend their handlers, and guard suspects.	○	○

Activity 2

Which statement best describes the mission of security forces? Select the best answer.

- ○ To secure Department of Defense buildings inside and out
- ○ To monitor facility access in the interest of national security
- ○ To protect Department of Defense assets
- ○ To protect key Department of Defense officials

Lesson Conclusion

In this lesson, you learned about the use of security forces, the ways in which security forces are deployed, and the types of DoD security forces. DoD security forces include government security forces, both military and civilian, contract security forces, and military working dogs. These security forces all work together to protect our nation's DoD assets.

Answer Key

Activity 1

	True	False
Government security forces may be either military or civilian.	●	○
Contract security forces may be either military or civilian.	○	●
Military working dogs can seek, detect, defend their handlers, and guard suspects.	●	○

Activity 2

The mission of all government security forces, civilian or military, contract forces, and military working dogs is to protect DoD assets.

Student Guide

Course: Physical Security Measures

Lesson 5: Security Technology and Equipment

Lesson Introduction

The final layer of physical security protection covered in this course is our security equipment and technology. This includes intrusion detection systems and equipment; closed circuit television, or CCTV; access control systems and procedures; and screening equipment.

The lesson objectives are:

- Identify the types of intrusion detection systems and equipment, as well as the purposes of and uses for each type
- Define closed circuit television (CCTV) and identify the purpose of and uses for CCTV
- Identify the types of access control systems and the purposes and uses for each type
- Identify the types of access control procedures and the purposes and uses for each type
- Identify the types of screening equipment and the purposes and uses for each type

Intrusion Detection Systems

1. Overview

The purpose of an Intrusion Detection System (IDS) is to deter, detect, and document intrusion. The IDS must detect an attempted or actual unauthorized entry into a protected environment, and is designed to complement other physical security measures.

An IDS does not prevent an intrusion. Rather, an IDS detects a change in the environment by a change of state of detection devices. This change of state of detection devices could be the result of an intruder or something else requiring further investigation.

These systems are a combination of components, including sensors, control or transmission units, transmission lines or wireless transmission devices, monitor units, and computerized monitoring stations. They are integrated to operate in a specific

manner and can be used indoors and outdoors. With the advent of modern-day electronics, the flexibility to integrate a variety of equipment and capabilities greatly enhances the potential to design an IDS to meet specific needs.

2. IDS Selection Factors

Some factors to consider when selecting an IDS include asset criticality, design considerations, environment, location, and perceived threat. Asset criticality helps define the degree of protection required, based on the importance of the asset to the mission. Asset criticality also helps define such factors as communication line security and security force response time requirements. Design considerations include construction of the building, room, or area being protected. Environmental considerations include electromagnetic interference, humidity, saltwater laden atmosphere, dust, weather conditions, animals, and insects. Location considerations include the geography, whether the area being protected is inside or outside a government installation or facility, and whether it is within or outside the continental United States. The perceived threat factor includes considerations of the degree of protection required to counter the threat including the level and type of criminal activity.

3. Operational Phases

The operational phases of an IDS are detection, reporting, dispatch, and response and assessment.

Detection begins as soon as a detector or sensor reacts to the stimuli it is designed to detect. The sensor alarm condition is then transmitted over cabling located within the protected area, called the detection loop, to the Premise Control Unit (PCU). The PCU may service many sensors. The PCU and the sensors it serves comprise an "alarmed area." The alarmed area may be reported by zones.

Reporting begins when the PCU receives signals from sensors in a protected area and incorporates these signals into a communications scheme. The signal is sent by the PCU via the transmission link to the monitoring station. A dedicated panel or central processor unit processes the signals and initiates an audible or visible alarm to the monitoring location. Alarms can result from intrusion, tampering, component failure, or system power failure, just to list a few.

The dispatch period is the first phase requiring human interaction. When an alarm condition occurs, the operator initiates the appropriate response such as dispatching the response force.

Response and assessment is initiated once a response force is dispatched and continues when they arrive at the scene of the alarm.

4. Types of IDS Monitoring

When an IDS is triggered, it sends an alarm to a monitoring point. Once the alarm notification is received, a response is required. You will now explore the three types of IDS monitoring. They are local, proprietary, and central station monitoring.

a. Local

An IDS with local alarm annunciation results in an audible and/or visual signal in the immediate vicinity only. Such systems afford limited protection and may be appropriate for lower priority resources. Response is by local on-site personnel or security forces notified of the alarm.

Some disadvantages of this type of monitoring system are that intruders know exactly when the alarm is activated and can easily avoid capture, there is no central monitoring, it may not provide immediate security force response, and there is no audit trail unless it is contained in the local PCU memory or on the local printer.

b. Proprietary Monitoring

A proprietary IDS is directly connected to an on-campus monitoring station. These systems normally do not transmit outside the campus area or organization. In these instances, local on-duty personnel receive the annunciation and initiate appropriate action. In most cases, intruders cannot hear the alarm, and therefore, are more likely to be captured.

The disadvantages of this type of monitoring system are that the stand-alone system may not have a back-up power system should the system go down, and that security force personnel may only become aware of the alarm when notified by the person monitoring the system.

c. Central Station Monitoring

A central station monitored IDS is remotely monitored by government or commercial resources. These resources maintain contact with an appropriate response force. The response force may be internal to the installation or facility, or a commercial source using local law enforcement personnel or private guards. Advantages include immediate notification, timely response by security or law enforcement personnel, and the possibility of back-up capability at the same location or another location.

Disadvantages include that Central Station Monitoring may involve large corporate monitoring agencies who do not fully understand the importance of a rapid response to alarms; the response times may exceed those required for

certain assets when using commercial response forces; and as the distance from the protected area to the monitoring station increases, the likelihood of a communications failure increases, potentially resulting in polling times exceeding the maximum of six minutes.

Intrusion Detection Equipment

1. Overview

Intrusion Detection Equipment (IDE) is a term used to describe the individual components of an IDS. These components are sensors and detectors, the Premise Control Unit (PCU), transmission line security, and a monitoring station, equipment, and personnel.

2. Sensors and Detectors

Sensors and detectors are devices that respond to a physical stimulus, such as a change of state, heat, light, sound, pressure, magnetism, or a particular motion.

Sensors and detectors are installed in various interior and exterior locations at an installation or facility.

You should take a variety of factors into consideration to select the appropriate sensor or detector. Exterior sensors or detectors must be reliable to withstand extreme outdoor temperatures, environmental concerns such as dust, rain, fog, snow, vibration, and natural debris, among others, and interference from animals or insects. Interior sensors or detectors must be reliable to withstand adverse effects caused by heating, ventilation, and air conditioning systems, and interference from animals or insects. Because the above interior and exterior factors may not be completely unavoidable, redundant systems using different types of sensors might be warranted to minimize false or nuisance alarms and promote system integrity.

There are many different types of sensors and detectors in use throughout the DoD. The table below lists some of the more commonly used types:

Sensor/Detector	Description
Balanced magnetic switch (BMS)/high-security switch	The BMS comprises a magnet assembly, reed switch, a small balancing magnet for gap and sensitivity adjustment, a tamper switch, and a resistor to signal any opens or shorts in that alarmed zone if that sensor is at the end of the line. The reed switch is held closed by the forces of a balanced magnetic field created between the operating magnet on the door and the internal balancing magnet. Movement of the door or window operating magnet, or moving another magnet close to the switch, causes it to activate the alarm.

Buried line sensor	A buried line sensor is, in essence, a disturbance sensor buried in the ground. A buried line sensor reacts to vibrations or pressures within a certain perimeter. These sensors are usually placed on the inside of a fenced area when one fence is used or between two fences when a double fence is used.
Capacitance sensor	These proximity devices act like antennas. When a person approaches or touches the object, its electrostatic field becomes unbalanced and triggers the alarm. Note: Only metal objects isolated from the ground can be protected this way.
Disturbance sensor	Disturbance sensors do just what their name implies. They are often used in conjunction with fences and detect any disturbance of the fence material, within specified parameters.
Electret cables	These cables are similar to coaxial cables, except that the material that surrounds the center wire has an electrical charge on it. When the cable is moved, the electrical charge is passed onto the center wire, thus changing the electrical current that runs through it.
Electric field sensor	An electric field sensor is composed of multiple wires; one has a current running throughout, and the other acts as a sensing mechanism. When something enters the electromagnetic field that is in the wire, the energy in the wire is disturbed and activates an alarm.
Electromechanical switch	These sensors contain either a series of ball-bearings or a liquid metal such as mercury, which forms a continuous electrical path. When the switch is moved, the ball bearings or liquid metal moves and contact with the internal terminals is broken, thus causing a change in the electrical current that passes through the sensor.
Geophone	These sensors have a magnet inside a coil. When the sensor is moved, the magnet moves. The movement of the magnet affects the current, which passes through the coil that is wound around the magnet.
Grid wire lacing	Thin foil or fine brittle wire sensor breaks electrical circuit.
Inertia detector	An inertia detector is attached to a protected surface that detects shock waves created by a seismic or inertial impact against that surface.
Microwave (high-frequency radio waves)	This sensor uses microwave energy to perform its job. It has a transmitter and a receiver. When the receiver detects a change in the microwave energy it is receiving from the transmitter, the alarm is activated.
Passive infrared (PIR)	A PIR sensor detects changes of infrared energy in its field of view.
Photoelectric	A photoelectric sensor is an instrument consisting of two units in which a light beam is transmitted from one of the units and is

	received by the other. It activates the alarm only when the beam is broken.
Piezoelectric transducers	These sensors are composed of a crystalline-type substance whose electricity-conducting property is changed when the sensor is moved.
Taut wire switch	A taut wire switch is attached to a fence or other type of barrier and detects a change in the tension of the wire.
Ultrasonic	Movement through sound waves saturating an area results in an alarm. These sound waves are above the range of human hearing.
Window break sensor	This sensor is a device bonded to a glass surface or attached to a window frame that senses an attack on that surface. The sensor may be either mechanical or audio. Audio glass break sensors may be installed on ceilings or walls to detect glass breakage within a range of the device. Window film, blinds, or curtains may reduce or prevent activation of this sensor.

3. Premise Control Unit (PCU)

The Premise Control Unit (PCU) is essentially the "brain" of the IDS. It is the centralized device that receives changes of state from IDE sensors, and transmits an alarm or trouble condition to the monitoring station.

The PCU is located inside the perimeter of the alarmed area. It is secured with a locking device, and is usually protected by an anti-tamper device.

The PCU should also contain a battery stand-by power source. The duration of stand-by protection varies depending upon the level of risk or applicable standards.

4. Transmission Security Line

The goal of transmission line security is to adequately supervise and protect the communications between the alarmed area and the monitoring station to prevent modification and substitution of the transmitted signal.

In high security areas, 128 bit or higher National Institute of Standards and Technology (NIST) listed encryption may be required. Transmission line security is determined and dictated by the type of DoD asset being protected.

The methods used to communicate alarm signals are digital dialer communication over standard telephone switched network, cellular dialer communication over the cellular network, two-way radio, direct connect, and data network or the Internet. The first two methods do not provide any line security. Two-way radio normally provides line security if polling is employed at least every six minutes. Polling time should be as short as possible, ideally as frequently as every few seconds. With direct connect, line security or

encryption may or may not be employed. A data network or the Internet provides line security when polling is provided at least every six minutes. Encryption of 128 bit or greater provides increased line security.

5. Monitoring Station, Equipment, and Personnel

A monitoring station is the central point for collecting the alarm status from the PCUs handling the alarms under the control of an IDS. Some important considerations in planning for your monitoring station are alarm zones, staffing, and response levels.

Alarms may be grouped into zones based on design or location depending on the sensitivity of the asset being protected. This is an important consideration during the design phase of your IDS installation.

Staffing of monitoring stations is another important consideration. Staffing requirements, such as security clearance, citizenship, and training, will be dictated by the criteria set by the appropriate authority. The importance of properly trained monitoring station personnel cannot be overstated. It is essential for these personnel to thoroughly understand system monitoring and operations to ensure that alarms are properly activated, areas are protected, and appropriate alarm response is initiated.

All alarms require some level of response. Alarms can be the result of an actual intrusion, or they may be activated due to a nuisance alarm or false alarm. Nuisance or false alarms may require a system maintenance, adjustment, or selection of an alternate sensor or detector. It is equally important for the owner or user of the protected area to be properly trained on system operations to ensure that alarms are properly activated and deactivated. Applicable authority will define the owner's or user's responsibilities.

Closed Circuit Television

1. Overview

CCTV plays a very important role in our physical security mission. Using CCTV is an excellent means for deterring and detecting loss, theft, or misuse of government property and resources, as well as unauthorized entry.

The recordings on the CCTV may provide evidence of these security breaches.

CCTV is used in a variety of facilities, installations, and activities, in areas ranging from some of our most sensitive DoD assets, through and including commissaries and exchanges, where they are used as a means to prevent, deter, and detect pilferage.

Security personnel are able to monitor multiple areas simultaneously, thereby saving manpower. Through the use of CCTV, we augment our existing security force, rather than replace it.

2. Features and Benefits

CCTV is simply a closed circuit television system with a camera that captures a visual image, converts it to a video signal and transmits it to a central monitoring station. There it can be received, displayed, recorded, and printed. The camera may record in color or black and white and may include remote control features such as pan, tilt, and zoom.

The signal transmission may be hard-wired or wireless. The monitoring equipment may be a single screen or a split screen. The recording equipment may be digital or tape. However, repeated use of the same tape can degrade the quality of the recorded images.

CCTV is versatile and can be installed inside or outside. However, you must consider environmental factors when selecting a system. In some instances, a camera may capture activity missed by security force personnel or details that guard force personnel may not be able to readily observe. CCTV enhances security by providing a real-time video surveillance and a means of video assessment of alarms.

3. Uses of CCTV

When installing an interior CCTV system, consideration should be given to using an IDS with the CCTV, such as a balanced magnetic switch or a high-security switch on a door to activate the camera when the door is opened. The IDS notifies the operator to view the monitor. This may reduce the number of video monitors required to view the protected areas.

When combined with video motion detection, CCTV can act as an IDS. The system processes the video signal from cameras and determines if a change has occurred in the camera's coverage. Video motion detection systems have the capability to mask out portions of a scene to decrease the number of nuisance alarms.

A CCTV system can also be a key asset in the event of a disaster. It may be used to show how an area looked before the event as well as after the event. In such cases, it can document valuable resources that were destroyed and can serve as a deterrent to looters.

The importance of properly trained CCTV monitoring personnel cannot be overstated. Remember, a CCTV is only as good as the people who operate it. Therefore, procedures must be in place and personnel must be trained in its use.

Access Control System

1. Overview

Access control is a process for allowing authorized personnel into a controlled area while preventing unauthorized personnel from entering the area. Throughout this lesson, the term "controlled area" may refer to installation, building, or controlled space.

There are different types of access control systems, from very simplistic manual systems, to more costly automated electronic systems.

The type of access control is usually determined based on risk management. Some systems, such as metal, radiological, or explosive detectors, are used in conjunction with manual entry control systems to enhance established security procedures. These systems serve to provide assurance that only authorized personnel and materials are introduced into or removed from a protected area.

Note that the Joint Personnel Adjudication System (JPAS) is not an access control system; rather, it is a system used to verify the level of access eligibility for specific individuals. Now let's look at the various types of access control systems.

2. Manual Systems

There are several manual control systems being used for access to various controlled areas in the DoD. The basic manual access control system is simply personal recognition. This may be employed where a small number of employees are involved. These employees must be trained to recognize and respond to the presence of unauthorized personnel. Another form of manual access control is a person who verifies an acceptable form of identification such as the Common Access Card (CAC).

Note: The Common Access Card (CAC) is the Department of Defense's implementation of smart card technology. A smart card is a credit card size device, normally for carrying and use by personnel that contains one or more integrated circuits and also may employ one or more of the following technologies: magnetic stripe, bar codes, non-contact and radio frequency transmitters, biometric information, encryption and authentication, or photo identification.

The DoD uses the CAC to meet the requirements of Homeland Security Presidential Directive 12, or HSPD-12. The number of different types of identification media is being reduced, relying heavily on the common identification criteria mandated by HSPD-12. Some facilities, depending on sensitivity of the area, may still require additional enhancement measures for entry.

Issued in August 2004, Homeland Security Presidential Directive-12 (HSPD-12) mandates a common Federal ID standard for all employees and contractors.

Note: The Common Access Card (CAC) is a controlled item and shall not be used in temporary badge issuance exchanges. Use of a badge such as an intelligence community badge as an identifying badge instead of an access credential is not prohibited in restricted areas by FIPS 201-1 or this regulation.

Some examples of additional measures are comparing a valid form of identification to an access roster or JPAS, a badge exchange program whereby one type of identification or badge is exchanged for one displayed within the controlled area, and a cipher access control device, which is either manual or electronic. These devices require the user to know a 3- or 4-digit number in order to gain access. The common forms are the push button cipher and keypad operated cipher.

One concern with badge systems is the requirement to reissue all badges based upon a percentage of lost or missing badges. Mass reissuing of badges to all badge holders incurs a significant cost. This cost must be weighed against the risk of having unaccounted for badges in circulation. Another concern with badge systems is the holder's failure to report loss of a badge to the appropriate authority.

If manual access control systems do not meet the appropriate access requirements based on the sensitivity of the protected area, an automated access control system may be a better solution.

3. Automated Systems

Technology has provided many options in electronic automated access control systems. Some employ biometrics and some do not.

Some things to consider when selecting automated access control systems include reliability, file capacity, resistance to counterfeiting, enrollment time, throughput time, cost, and technical complexity. A final consideration is that automated control systems may lead to a false sense of security.

a. Non-Biometric

Card swipe, with or without a personal identification number (PIN) is an example of a non-biometric access control system. Likewise, in lieu of a card swipe reader, the same functionality can be achieved with a "proximity" card or key system. Both of these methods communicate with a computerized system, which allows for approval or denial of entry, based on programmed information provided by authorized personnel.

An extremely useful feature of these systems is their ability to enable entry at specific points for specific periods of time. The same concerns that apply to manual systems using badges also apply to non-biometric access control systems. One additional concern associated with PINs is users' loss or

compromise of their PINs. Loss of a card plus the loss of its associated PIN equals a potential breach of area security.

b. Biometric

Biometrics are measurable physical characteristics or personal behavioral traits used to recognize the identity, or verify the claimed identity, of an individual. Individually unique characteristics include fingerprints, hand geometry, handwriting, iris scan, and voice recognition. Technology has provided many options in biometric automated access control systems.

During the design analysis phases of biometric access control systems, error rates and cost must be considered. Some concerns associated with biometrics are that more data is required from the user and the validation time period is longer. There are also concerns over divulging personal characteristics. The benefits of biometric systems are a higher level of security and a possible reduction in security force personnel.

The most common individual biometric characteristics are fingerprints, hand geometry, handwriting, iris scan, and voice recognition.

Biometrics	Description
Fingerprints	Fingerprints have been used as a positive personnel identifier for more than 100 years. The art of processing human fingerprints for identification has been greatly enhanced in recent years by the development of automated systems. These systems, which rely on pattern recognition of either a single finger or several fingers and computerized data processing, have an application in access control. All fingerprint identification systems require accurate finger positioning and pattern measurement for reliable identification. Some problems occur with individuals who do not have clearly defined finger ridge patterns or who have had an injury to the identifying finger.
Hand Geometry	The measurement of relative finger length is a unique characteristic. Hand geometry is a distinct measurable and individual characteristic. These systems are characterized as having high to medium resistance to tampering.
Handwriting	Signature verification has been used for many years by the banking industry. However, signature comparison methods employed are highly susceptible to forgery. Automated handwriting verification systems have been developed that use handwriting dynamics such as velocity, acceleration, and pressure as a function of time. Statistical evaluation of this data indicates that an individual's signature is unique and reasonably consistent from one signature to the next. Systems have been developed that used from one to three

	axes of dynamic measurements. Transducers can be located in either the writing instrument or tablet. Like hand geometry, signature verification has a high to medium counterfeiting resistance level.
Iris Scan	Iris scanning systems measure the iris and are very difficult for the user to circumvent. More advanced systems use a charge-coupled device camera, which is unobtrusive and requires little action on the user's part. Because the scan involves shining a light into the eye, one potential problem with these devices is that they may irritate the user's eye if used on a routine basis. Employees have shown resistance to eye scanning systems for this reason.
Voice Recognition	Speech, or voice recognition, is a useful attribute for identity verification, and it is well suited to automated data processing. Speech measurements that are useful for speaker discrimination include waveform envelope, voice pitch period, relative amplitude spectrum, and vocal tract resonant frequencies (formats). High-end systems have a high resistance to counterfeiting; however, some low-end systems can be fooled with high-quality recordings.

Access Control Procedures

1. Overview

Access control procedures vary greatly among components, installations, and facilities. Identifying who and what enters the controlled areas is vital to protecting DoD assets.

You just learned about access control systems and now you will learn some procedures employed in the use of these systems. You will learn about methods of control, use of escorts, and entry and exit inspections.

2. Methods of Control

When individuals need access to a controlled area, access control is employed by security force personnel using automated or manual systems, or a combination of both.

With automated systems, the individual has been vetted and receives an appropriate DoD credential. Local authorities determine the level of monitoring of these automated systems. Individuals who fail to meet the access criteria will be referred to the next tier of screening.

With manual systems, the individual may or may not have been pre-approved through an activity's vetting process. Let's look at some examples.

An individual has a CAC that serves as a DoD credential and is commonly used to gain access to DoD controlled areas. In this case, the individual is authorized unescorted access to the area.

An individual has a record in JPAS reflecting the proper level of access eligibility. In this case, the host may grant access if need-to-know is verified. Although JPAS access is verified, the individual may still require a visitor badge, either with or without an escort, as determined by the activity.

An individual does not have an approved DoD credential. However, the individual does have an official need to gain access in the performance of their duties. In this case, the individual may require a visitor badge, either with or without an escort, as determined by the activity.

With either system, follow-on processing and inspection may be required, as determined by local procedures.

3. Escort Requirements

Another access control procedure is the use of escorts. An escort is required when individuals visit areas for which they do not have unescorted access, the appropriate security clearance, and/or a valid need-to-know. For example, visitors may have the appropriate security levels, but not the need-to-know or access to special types of information protected within the controlled area. If access is approved, the visitor will sign in at the visitor center or security force post, show a valid photo identification, be issued an escort-required visitor badge that must be visually displayed during their visit, and be assigned an escort.

Escorts play a crucial role in asset protection within the controlled area. Their responsibility begins when the visitor enters the controlled area, and does not end until the visitor has departed. Escorts have the ultimate responsibility and must be able to control the visitor during the duration of their visit. One hundred percent accountability of visitors is mandatory!

The selected escort should be trained to their escort responsibilities, acknowledge receipt of training, be reliable, understand and conform to the identified practices and procedures, and understand the possible consequences if positive control of the visitor is not maintained.

Local directives will determine and dictate specific procedures that assigned escort personnel must follow.

4. Entry and Exit Inspections

Entry and exit inspections are an essential component of the physical security program.

They help prevent or deter the introduction of unauthorized or prohibited material into an installation or facility, and also are valuable in the detection of assets being removed from an installation or facility without proper authorization. Inspections of vehicles,

personnel, or their property, conducted either randomly or during periods of increased alertness, greatly increase the likelihood of detecting unauthorized or prohibited items.

The schedule for conducting these types of inspections should be limited to senior officials and security personnel. After consultation with legal personnel, installation and facility authorities determine the criteria for conducting inspections of individuals, material in their possession, and vehicles, whether random or continual 100% of the time. Local guidance will dictate the means used to notify individuals that they may be subject to inspections.

Screening Equipment

1. Overview

Security screening equipment at DoD installations and facilities has become more common since the terrorist attacks on the Murrah Federal Building in Oklahoma City in April 1995 and the attacks of September 11, 2001.

Security screening equipment adds greatly to our ability to protect DoD assets by screening personnel and property to identify potentially dangerous and unauthorized items. Detection of unauthorized or prohibited items is enhanced through manufacturer-required calibration and formal operator training. Realistic refresher training using simulated unauthorized material also enhances the detection of unauthorized or prohibited items.

The two types of screening equipment most frequently used by the DoD are fixed and portable security screening equipment. Let's examine each more closely.

2. Fixed

Fixed security screening equipment includes a variety of types such as conveyor belt style x-ray machines, magnetometers configured for pedestrian traffic, and emerging technologies with the ability to detect explosive residue.

X-ray machines have proven to be an effective means to detect and deter the movement of dangerous or prohibited items into areas like airports, federal buildings, and DoD facilities, activities, and installations. When employed, this is accomplished by requiring that hand-carried items be presented for inspection by screening equipment.

Threats to security come in many different forms, and x-ray machines are an effective way to screen what people bring into a facility. However, not all threats to security are clearly visible using x-ray machines. Therefore, additional physical screening may be appropriate.

Magnetometers, commonly referred to as metal detectors, are a means to screen personnel for unauthorized or dangerous metal objects. They do this by creating a magnetic field. When this magnetic field is disturbed by a metal object, it triggers an alarm. An appropriate response to the alarm is hand screening, using portable screening equipment, or a manual search. Some harmless medically implanted devices may cause an alarm and may require hand screening before clearance is granted to enter the controlled area.

Naturally, placement of the equipment depends on the design of the facility, and the area or asset to be protected. Various types of channeling or funneling barriers can ensure screening of all personnel entering the protected area.

3. Portable

Portable security screening equipment can include items such as hand-held magnetometers, commonly referred to as wands, and vapor trace detectors.

Wands may be used as a back-up for fixed screening equipment to determine the cause of the alarm. Wands may also be the only screening equipment available at some facilities or installations. Like all magnetometers, wands use a magnetic field, which causes an audible alarm when disturbed by a metal object. Based on the size of the object and the sensitivity setting of the device, there may or may not be a detection.

Vapor trace detectors are extremely sophisticated pieces of equipment used to detect minute traces of the chemicals associated with explosive materials.

Review Activity

Try answering the following questions. When you are finished, see the Answer Key at the end of this Student Guide to check your answers.

Activity 1

Match each description to the type of IDS to which it applies. Check your answers in the Answer Key at the end of this Student Guide.

Description	Type of IDS
A. Responds to a physical stimulus B. Receives change of state and transmits alarm C. Central point for collecting alarm status D. Assures communications between the alarmed area and the monitoring station	___ Sensor/detector ___ Transmission line security ___ Premise Control Unit (PCU) ___ Monitoring station

Activity 2

Select True or False for each statement.

	True	False
A CCTV camera may capture activity missed by security force personnel.	○	○
A CCTV can act as an intrusion detection system (IDS) when combined with video motion detection.	○	○
An advantage of CCTV is that environmental factors do not affect its performance.	○	○
A CCTV is only as good as the people who operate it.	○	○

Activity 3

Which of the following are access control systems? Select all that apply.

- ☐ Closed circuit television
- ☐ Card-swipe system
- ☐ Joint Personnel Adjudication System (JPAS)
- ☐ Badge exchange program
- ☐ Personal recognition
- ☐ Iris scanning
- ☐ Intrusion detection system

Activity 4

Select True or False for each statement.

	True	False
Escorts must be able to control the visitor they are escorting throughout the duration of their visit in a controlled area.	○	○
The schedules for entry and exit inspections should be posted in view of all DoD personnel.	○	○
All visitors with the appropriate access level to enter a controlled area are permitted unescorted entry.	○	○
Entry and exit inspections help deter the introduction of unauthorized or prohibited material into an installation or facility and help prevent the unauthorized removal of DoD assets from an installation or facility.	○	○

Activity 5

Match each description to the type of screening to which it applies. Check your answers in the Answer Key at the end of this Student Guide.

Description		Type of Screening
A. Fixed equipment that detects metal objects	___	Magnetometer
B. Detects traces of explosive material	___	Vapor trace detector
C. Portable equipment that detects metal objects	___	Wand
D. Detects prohibited items	___	X-ray machine

Lesson Conclusion

In this lesson you learned about intrusion detection systems and equipment, closed circuit television (CCTV), access control systems and procedures, and screening equipment.

Answer Key

Activity 1

Description		Type of IDS
A. Responds to a physical stimulus B. Receives change of state and transmits alarm C. Central point for collecting alarm status D. Assures communications between the alarmed area and the monitoring station	_A_	Sensor/detector
	_D_	Transmission line security
	_B_	Premise Control Unit (PCU)
	_C_	Monitoring station

Activity 2

	True	False
A CCTV camera may capture activity missed by security force personnel.	●	○
A CCTV can act as an intrusion detection system (IDS) when combined with video motion detection.	●	○
An advantage of CCTV is that environmental factors do not affect its performance.	○	●
A CCTV is only as good as the people who operate it.	●	○

Activity 3

- ☐ Closed circuit television
- ☒ Card-swipe system
- ☐ Joint Personnel Adjudication System (JPAS)
- ☒ Badge exchange program
- ☒ Personal recognition
- ☒ Iris scanning
- ☐ Intrusion detection system

Activity 4

	True	False
Escorts must be able to control the visitor they are escorting throughout the duration of their visit in a controlled area.	●	○
The schedules for entry and exit inspections should be posted in view of all DoD personnel.	○	●
All visitors with the appropriate access level to enter a controlled area are permitted unescorted entry.	○	●
Entry and exit inspections help deter the introduction of unauthorized or prohibited material into an installation or facility and help prevent the unauthorized removal of DoD assets from an installation or facility.	●	○

Activity 5

Description		Type of Screening
A. Fixed equipment that detects metal objects B. Detects traces of explosive material C. Portable equipment that detects metal objects D. Detects prohibited items	_A_	Magnetometer
	_B_	Vapor trace detector
	_C_	Wand
	_D_	X-ray machine

Student Guide

Course: Physical Security Measures

Lesson 6: Course Conclusion

Course Summary

Physical security measures are designed to prevent or reduce the potential for sabotage, theft, trespassing, terrorism, espionage, or other criminal activity. To ensure security, the security measures must provide the capability to deter, detect, identify, track, assess, record, communicate, delay, and respond to unauthorized access activities. Security operations and procedures must ensure the effective protection of Department of Defense (DoD) assets.

In this course, you learned about the application of active and passive complementary physical security measures to achieve security-in-depth and to protect DoD assets from potential threats.

Lesson Review

Here is a list of the lessons in the course:

- Security-in-Depth
- Exterior Physical Security Measures
- Security Forces
- Security Technology and Equipment

Course Objectives

You should now be able to:

- ✓ Identify key concepts related to security-in-depth
- ✓ Identify the various types of physical security measures and their uses

Conclusion

Congratulations. You have completed the Physical Security Measures Course.

To receive credit for this course, you must take the Physical Security Measures examination. Please use the Center for Development of Security Excellence Learning Management System STEPP to register for the online exam.