Student Guide

Course: Physical Security Planning and Implementation

Lesson 1: Course Introduction

1. Course Information

Purpose	Provide a thorough understanding of physical security planning and implementation within the DoD
Audience	Military, civilian, and contractor personnel responsible for physical security
Pass/Fail %	75% on final examination
Estimated completion time	145 minutes

2. Course Overview

Planning for the physical security of Department of Defense (DoD) installations and resources is imperative for our national security.

In this course, you will learn about various components of physical security planning and implementation. These components include physical security roles; the risk management model; facility design; physical security planning documents; the DoD Antiterrorism Program, which includes Terrorist Threat Levels and Force Protection Conditions (FPCONs); and the oversight of the physical security program.

3. Course Objectives

Here are the course objectives:

- Identify the components of physical security planning and implementation
- Identify the roles in physical security
- Identify the components of the risk management model
- Identify what Terrorist Threat Levels are and who establishes them
- Identify what Force Protection Conditions are and who establishes them
- Identify physical security protective measures that should be incorporated into new and existing facility design
- Identify physical security planning documents and their purposes, including a facility's physical security plan
- Identify the purpose of oversight and the oversight tools

4. Course Structure

This course is organized into the lessons listed here:

- Course Introduction
- What is Physical Security Planning and Implementation?
- Facility Design
- Physical Security Planning Documents
- DoD Antiterrorism Program
- Oversight
- Course Conclusion

Student Guide

Course: Physical Security Planning and Implementation

Lesson 2: What is Physical Security Planning and Implementation?

Lesson Introduction

1. Objectives

This lesson will familiarize you with a variety of concepts related to physical security planning and implementation in the Department of Defense (DoD), including the risk management process and the various roles involved in the planning and implementation of physical security.

Lesson objectives:

- Identify the components of physical security planning and implementation
- Identify the components of the risk management model
- Identify the roles in physical security

2. Overview

Physical security planning is deciding which security measures will be used to prevent unauthorized access to DoD assets and to safeguard those assets against threats such as espionage, sabotage, terrorism, damage, and criminal activity. In physical security planning, the risk management process is used to provide a systematic approach to acquiring and analyzing the information necessary for protecting assets and allocating security resources against the threats.

Physical security implementation is the execution of physical security plans, including the oversight and inspection process, which ensures those plans are properly implemented.

3. Policy

The DoD has implemented several DoD-wide policy documents that guide DoD physical security planning and implementation, such as:

- DoD 5200.08-R, Physical Security Program
- DoD Instruction (DoDI) 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)
- DoD Directive (DoDD) 3020.26, DoD Defense Continuity Program
- DoDI 2000.12, DoD Antiterrorism Program
- DoDI 2000.16, DoD Antiterrorism Standards
- DoD Antiterrorism Officer Guide

- DoDM 5200.01 DoD Information Security Program

The Army, Navy, Marine Corps, and Air Force issue specific implementation guidance for their individual service branches. You should always consult your component's policy for specific guidance.

Physical Security Planning

1. Risk Management Process

In order to plan and implement effective physical security measures, you must use the risk management process to determine where and how to allocate your security resources. The steps in the risk management process are: assess assets; assess threats; assess vulnerabilities; assess risks; determine countermeasure options; and make risk management decisions.

For in-depth training on the risk management process, refer to the Risk Management for DoD Security Programs eLearning course offered by DSS Center for Development of Security Excellence.

a. Assess Assets

Properly designed and executed physical security programs should deter or prevent, to the greatest degree possible, the loss of, theft of, or damage to an asset. DoD assets include people, information, equipment, facilities, activities, and operations. Combined, these assets are referred to as PIE-FAO. When assessing an asset, you must determine the nature and value of that asset and the degree of impact if the asset is damaged or lost.

b. Assess Threats

Next you must identify and assess the threats to those assets. A threat can be an indication, circumstance, or event with the potential to cause loss of, or damage to, an asset or capability. Examples of threats include threats from the Foreign Intelligence Entities, criminal activities, insider threats, terrorist organizations, cyber threats, and business competitors.

c. Assess Vulnerabilities

Next you must identify the vulnerabilities, or situations or circumstances, which if left unchanged, may result in the degradation, loss of life, or damage to mission-essential resources, and determine their extent. Vulnerabilities are weaknesses, characteristics, or circumstances that can be exploited by an adversary to gain access to or information from an asset. Vulnerabilities can be the result of a variety of factors, such as the way a building was constructed, location of people, equipment, operational practices, and even personal behavior.

d. Assess Risks

Once you have identified your assets, threats, and vulnerabilities, you must then assess your risks. Think about the impact if your assets are being compromised, such as loss of strategic or military advantage or even loss of life.

e. Determine Countermeasure Options

Once you've calculated the risks, you must determine which countermeasures you might employ to protect our DoD assets by reducing our vulnerabilities and mitigating our threats. Countermeasures include what security measures you employ up front in facility design, in the day-to-day protection of DoD assets, and in times when threat levels increase.

f. Make Risk Management Decisions

Once you've determined your countermeasure options, you must make risk management decisions based on the cost versus the benefit of protecting DoD assets.

2. Activities

Several activities comprise the physical security planning phase. Physical security planning must begin with the design of any facility, installation, or mission. Including physical security measures in the design phase is critical to the protection of mission capabilities and is essential for an effective physical security program.

Physical security planning includes the creation of written plans, such as the Physical Security Plan, Standard Operating Procedures, and Post Orders. Experience has proven that by establishing written plans, all people involved understand their roles, responsibilities, and procedures both in the day-to-day physical security program as well as in the event of an emergency.

Physical security planning also includes antiterrorism, or AT, planning, which is planning for the defensive measures to be used to reduce the vulnerability of individuals and property to terrorist attacks.

Physical Security Implementation

1. Activities

Physical security implementation occurs in a variety of ways. When you incorporate physical security measures in the construction or renovation of facilities according to the facility design plans, you are implementing physical security.

The various physical security planning documents are used to implement physical security measures both on a day-to-day basis and in emergency situations.

When implementing antiterrorism measures, the DoD uses Terrorist Threat Levels and Force Protection Conditions to communicate levels of threat in specific areas and what security measures are to be used in response to those threats.

To ensure the appropriate implementation of physical security measures, you can use a variety of oversight tools. These tools include day-to-day observations, surveys, staff assist visits, inspections, and analysis of reports.

You will learn more about each of these topics later in this course.

Physical Security Roles

1. Groups Involved in Physical Security

Physical security is not about one entity taking care of everything, but rather an integrated and coherent effort for the protection of national security and other DoD assets. There are several groups and individuals involved in physical security planning and implementation. As a physical security specialist, you will assume some of these roles, serve on many of these working groups, and interact with others. The groups involved in physical security planning and implementation include the Antiterrorism Working Group (ATWG), Information Systems Security Managers (ISSMs), Legal Officers, the Threat Working Group (TWG), and the Defense Critical Infrastructure Program (DCIP) working group.

a. ATWG

As outlined in DoD Instruction (DoDI) 2000.16, DoD Antiterrorism Standards, the Antiterrorism Working Group (ATWG) meets at least semi-annually and oversees the implementation of the Antiterrorism (AT) program that protects DoD assets against terrorism. They accomplish this by developing and refining AT plans and addressing emergent or emergency AT Program issues. The ATWG comprises the Antiterrorism Officer (ATO), the Installation Commander or designated representative, representatives of the principal staff, including a chemical, biological, radiological, nuclear, and high yield explosive representative, tenant unit representatives, and others as directed by Installation Commanders.

b. ISSMs

The Information Systems Security Managers (ISSMs) are responsible for the security of information systems. They coordinate physical security measures and develop contingency plans for the protection of the information systems.

c. Legal Officers

Legal Officers work closely with the Antiterrorism Officer and others to ensure that security considerations are properly and legally incorporated into the physical security plan.

d. TWG

As outlined in DoD Instruction (DoDI) 2000.16, DoD Antiterrorism Standards, the Threat Working Group (TWG) meets at least quarterly and is responsible for developing and refining terrorism threat assessments based on the threats against DoD assets. The TWG also coordinates and disseminates threat warnings, reports, and summaries. This group comprises an Antiterrorism Officer, the Installation Commander or designated representative, members of the staff, tenant unit representatives, law enforcement representatives, and the Intelligence Community (IC).

e. DCIP

As outlined in Department of Defense Directive (DoDD) 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, the Defense Critical Infrastructure Program (DCIP) working group is responsible for developing and providing installation Critical Infrastructure Protection (CIP) policy, program execution, and oversight recommendations, which include identifying and prioritizing mission essential critical assets and infrastructures and assessing their vulnerability and risk to human error, natural disasters, or intentional physical or cyber attack. This group also develops strategies for remediating or mitigating vulnerabilities and risks to critical assets and infrastructures.

The information in the box below will not be on the test, but it may provide you with useful background and insights.

The Antiterrorism (AT) program is one of several security-related programs that fall under the overarching Combating Terrorism and Force Protection programs. The AT program is a collective, proactive effort focused on the prevention and detection of terrorist attacks against DoD personnel, their families, facilities, installations, and infrastructure critical to mission accomplishment as well as the preparation to defend against and planning for the response to the consequences of terrorist incidents. Although not elements of AT, plans for terrorism consequence management preparedness and response measures as well as plans for continuing essential military operations are important adjuncts to an effective AT program. The minimum elements of an AT program are AT risk management, planning, training and exercises, resource application, and a program review.

2. Individuals Involved in Physical Security

The agencies and organizations that protect our national security and DoD assets are comprised of individuals who play an important part in the mission of physical security. These individuals include the Installation Commander or Facility Director; the Antiterrorism Officer (ATO); Counterintelligence (CI) support personnel; local, state, and federal law enforcement officials; the Operations Security (OPSEC) Officer;

the Physical Security Officer; the Defense Critical Infrastructure Program (DCIP) Officer; and the Civil Engineer.

a. Installation Commander/Facility Director

Installation Commanders or Facility Directors are responsible for several aspects of physical security. These responsibilities include the safety and protection of the people and property under their command; planning, forming, coordinating, and integrating all physical security matters into their installation; and identifying mission essential capabilities.

Department of Defense Instruction (DoDI) 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB), authorizes commanders to issue regulations for the protection and security of property or places under their command and to take reasonably necessary and lawful measures to maintain law and order and to protect installation personnel and property.

b. ATO

The Antiterrorism Officer (ATO) manages the installation or facility Antiterrorism (AT) program. This program uses defensive measures to reduce the vulnerability of individuals and property to terrorist attacks.

c. CI Support Personnel

Counterintelligence (CI) support personnel are vital to supporting the physical security mission. They are responsible for providing information on the capabilities, intentions, and threats of our adversaries. They must pay particularly close attention to those adversaries associated with foreign intelligence entities. In addition, CI support personnel are there to provide valuable assessments of counterintelligence considerations in support of physical security programs.

d. Law Enforcement Officials

Local, state, and Federal law enforcement officials are vital to the physical security program. Effective liaison with these officials fosters good working relationships so we can coordinate antiterrorism concerns and efforts, prepare an emergency response, and address criminal incidents. Coordination activities support mutual understanding of jurisdiction and authority.

e. OPSEC Officer

The Operations Security (OPSEC) Officer is an integral part of the physical security team. These individuals facilitate the process for identifying critical information, identifying threats to specific assets, assessing vulnerabilities to assets, analyzing risk to specific assets and to national security as a whole, and assist in developing countermeasures against potential threats to national security and other DoD assets.

f. Physical Security Officer

The Physical Security Officer is charged with managing, implementing, and directing physical security programs. This person may also be responsible for the development and maintenance of physical security plans, instructions, regulations, and standard policies and procedures. He or she may also coordinate with local law enforcement agencies, antiterrorism officers, and loss prevention personnel. The Physical Security Officer also conducts inspections and performs other oversight activities.

g. DCIP Officer

The Defense Critical Infrastructure Program (DCIP) Officer is responsible for carrying out the DCIP mission within a given installation or facility. The DCIP Officer is responsible for the identification, assessment, and effective risk management of Defense Critical Infrastructure (DCI) assets essential to mission success of a given installation or facility. This person also collaborates with DCI asset owners and public and private-sector activities essential to mission success of a given installation or facility. Examples of DCI assets include power grids, network hubs, and transportation lanes.

h. Civil Engineer

As part of Security Engineering Facilities Planning, the Civil Engineer provides planning, design, and support to physical security, force protection, and antiterrorism programs at installations. The Civil Engineer evaluates, manages, and develops design criteria for DoD physical security projects in accordance with DoD Security Engineering concepts and standards contained in the Unified Facilities Criteria (UFC).

Those design criteria include the assets that should be protected; the threats to those assets in terms of the potential aggressor tactics and their associated weapons, tools, explosives, and agents; the levels to which those assets should be protected against the threats; how those criteria, in combination with building types and some limited site information can be used to develop a planning level cost estimate for mitigating the effects of the threat; and how the design criteria may impact project scope.

Review Activity 1

Which of the following statements are true of physical security planning and implementation? Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

- ☐ The risk management process must be used to plan which physical security measures should be utilized to protect DoD assets.
- ☐ Protection of DoD assets must be performed at any cost; therefore, a cost vs. benefit analysis is not necessary.
- ☐ Use of oversight tools is an important part of physical security implementation.
- ☐ Facility design must be considered in physical security planning.

Review Activity 2

Select the best answer. Then check your answers in the Answer Key at the end of this Student Guide.

	Terrorist	**Fence**	**Open, unattended installation gate**	**Arms and ammunition**	**Loss of life**
Which of the following would best be described as a DoD asset?	○	○	○	○	○
Which of the following would best be described as a threat?	○	○	○	○	○
Which of the following would best be described as a vulnerability?	○	○	○	○	○
Which of the following would best be described as a risk?	○	○	○	○	○
Which of the following would best be described as a countermeasure?	○	○	○	○	○

Review Activity 3

Select the appropriate words from the Word Bank to complete the statements below. Then check your answers in the Answer Key at the end of this Student Guide.

Word Bank
A. Law Enforcement
B. Antiterrorism Officer
C. OPSEC Officer
D. CI Support
E. Physical Security Officer
F. DCIP Officer
G. Installation Commander/ Facility Director

1. The **[blank]** is responsible for the installation's antiterrorism program.
2. **[blank]** is responsible for providing valuable information on the capabilities, intentions, and threats of adversaries.
3. The **[blank]** analyzes threats to assets and their vulnerabilities.
4. **[blank]** must be included in the intelligence gathering process so that they can be part of coordinating emergency responses and criminal incidents on a Federal installation.
5. The **[blank]** is charged with the management, implementation, and direction of all physical security programs.
6. The **[blank]** is responsible for the safety of people and property under their command.
7. The **[blank]** is responsible for mitigating risks against Defense Critical Infrastructure assets that support the mission of an installation or facility.

Answer Key

Review Activity 1

Which of the following statements are true of physical security planning and implementation?

- ☑ The risk management process must be used to plan which physical security measures should be utilized to protect DoD assets.

***Feedback**: True. Assets, threats, vulnerabilities, and risks must be identified before determining which physical security countermeasures to use.*

- ☐ Protection of DoD assets must be performed at any cost; therefore, a cost vs. benefit analysis is not necessary.

***Feedback**: False. Cost vs. benefit must always be considered when planning the protection of DoD assets.*

- ☑ Use of oversight tools is an important part of physical security implementation.

***Feedback**: True. Oversight tools—such as observations, surveys, and inspections—are important in ensuring that physical security is being implemented appropriately.*

- ☑ Facility design must be considered in physical security planning.

***Feedback**: True. Physical security countermeasures must always be planned for when designing a facility.*

Review Activity 2

Question	Answer	Feedback
Which of the following would best be described as a DoD asset?	Arms and Ammunition	*Arms and ammunition would be considered equipment assets in PIE-FAO, which stands for the following DoD assets: People, Information, Equipment, Facilities, Activities, and Operations.*
Which of the following would best be described as a threat?	Terrorist	*A terrorist is a threat to DoD assets.*
Which of the following would best be described as a vulnerability?	Open, unattended installation gate	*A gate to an installation that was inadvertently left open and unattended would be a vulnerability as that would make it easier for unauthorized access to the installation.*
Which of the following would best be described as a risk?	Loss of life	*Loss of life is a very important risk you must consider when planning for the physical security of an installation or facility.*
Which of the following would best be described as a countermeasure?	Fence	*A fence is one of many physical security countermeasures used to protect DoD assets.*

Review Activity 3

Word Bank
A. Law Enforcement
B. Antiterrorism Officer
C. OPSEC Officer
D. CI Support
E. Physical Security Officer
F. DCIP Officer
G. Installation Commander/ Facility Director

1. The **[blank]** is responsible for the installation's antiterrorism program. *Answer B, Antiterrorism Officer.*
2. **[blank]** is responsible for providing valuable information on the capabilities, intentions, and threats of adversaries. *Answer D, CI Support.*
3. The **[blank]** analyzes threats to assets and their vulnerabilities. *Answer C, OPSEC Officer.*
4. **[blank]** must be included in the intelligence gathering process so that they can be part of coordinating emergency responses and criminal incidents on a Federal installation. *Answer A, Law Enforcement.*
5. The **[blank]** is charged with the management, implementation, and direction of all physical security programs. *Answer E, Physical Security Officer.*
6. The **[blank]** is responsible for the safety of people and property under their command. *Answer G, Installation Commander/ Facility Director.*
7. The **[blank]** is responsible for mitigating risks against Defense Critical Infrastructure assets that support the mission of an installation or facility. *Answer F, DCIP Officer.*

Student Guide

Course: Physical Security Planning and Implementation

Lesson 3: Facility Design

Lesson Introduction

1. Objectives

The design of facilities and installations is critical to the protection of DoD assets. This lesson will familiarize you with the physical security protective measures that should be included in new DoD facility construction as well as in renovations.

Lesson objective:

- Identify physical security protective measures that should be incorporated into new and existing facility design

Physical Security and Facility Design

1. Purpose

Properly designed facilities protect DoD assets by providing a physical and psychological deterrence to intruders such that the risk of intruding would be easily exposed. The design alone, plus additional security measures, can make a facility a hard target for adversaries. On the other hand, soft target facilities are typically identified as having minimal or no security measures, which may leave little or no evidence of a breech in security. You will find physical security planning, system acquisition, construction, and leasing standards in DoD 5200.08-R, Physical Security Program. When deciding which physical security measures to include in your facility design, there are other factors you must consider. These considerations include assessing the risks to your assets, costs associated with acquiring and maintaining the physical security measures, functionality and interoperability of the security measures, as well as future enhancements.

The information in the box below will not be on the test, but it may provide you with useful background and insights.

Hard targets include installations, facilities, or activities that provide a physical and psychological deterrence to intruders through the use of physical security measures.

Soft targets include installations, facilities, or activities with little or no security measures so it is easy to breech their security.

2. Physical Security Measures

The first line of defense in any facility is usually some form of perimeter protection system. The perimeter of an installation or facility is the outermost area of responsibility. Barriers, fences, and lighting are integral parts of this protection system. Another line of defense includes intrusion detection systems (IDS), access control systems, closed circuit television (CCTV), and barring man-passable openings.

For a more detailed look at each of these physical security measures, refer to the Physical Security Measures eLearning course offered by DSS Center for Development of Security Excellence (CDSE). For the specifications of these security measures, refer to Military Handbook 1013/1A, Military Handbook 1013/10, and specific DoD component guidance. Let's take a look at how each of these physical security measures protects an installation or facility.

Barriers

1. Purpose

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. Appropriately designed and located barriers are required to delay a forced entry threat or to stop a standoff, ballistic, or vehicle bomb attack. In the case of forced entry, the delay must be sufficient to allow the system time to detect, assess, and react appropriately. Barriers are also used to define boundaries and channel traffic through designated access control points where pedestrians, vessels, and vehicles can be monitored and searched for prohibited items.

2. Types

Barrier systems are considered active if they require action by personnel or equipment to permit entry to personnel or vehicles. Examples of active barriers include manually or electronically operated gates or turnstiles and hydraulic pop-up vehicle barriers.

Passive barriers rely on their bulk or mass to be effective and they have no moving parts. Examples of passive barriers include perimeter or vehicle barriers, temporary barriers, building perimeter barriers, and interior barriers.

Natural barriers are topographical features that assist in impeding or denying access to an area. Examples of natural barriers are rivers, cliffs, canyons and dense growth.

3. Considerations

You must consider various factors when deciding which types of barriers to use as physical security measures on your installation or facility:

- Do they need to be crash-rated to resist a vehicle's attempt to crash through them? Having a crash rating will increase the cost of the barrier, so cost must also be considered.
- Does the barrier need to be aesthetically pleasing?

Whatever type of barrier you decide to use, you must ensure that the installation or facility has the proper equipment to move the barriers when necessary. And you must ensure that the barriers are located in such a way that they do not block handicap access or emergency response vehicles.

Fencing

1. Purpose

Fencing is a vital part of your physical security program. Fences define a particular area, such as a military installation, and provide legal evidence of intent. They hold up signs and protect bulky assets. Finally, fences control both vehicular and pedestrian traffic, which prevents inadvertent entry and delays unauthorized entry.

2. Types

The DoD uses different types of fencing materials, the most common of which is chain link fence. DoD specifications require that chain link fencing be constructed of 9-gauge or heavier galvanized steel mesh wire of no more than 2 inches in diameter, be at least 6 to 8 feet tall, and the bottom should be no more than 2 inches from the ground. While economical, a chain link fence alone does not afford as much protection as one equipped with top guards, also known as outriggers, and barbed or concertina wire or other enhanced security standards.

In addition to being used as supplemental protection on chain link fences, both barbed wire and concertina, also known as c-wire, can be used as standalone fences or barriers. Concertina wire comes in 50 foot length coils that can be either 12 or 60 inches high and are stackable. As a standalone barrier, concertina wire is commonly used in combat environments.

Barbed wire fencing is made of 12-gauge twisted double strand wire with four point barbs spaced 4 inches apart on top. The vertical distance between the strands of wire should be no more than 6 inches apart. Standalone barbed wire fencing posts should be at least 7 feet high with 4 feet above ground, should be made of wood at least 4 inches in diameter, and should be spaced no further than 10 feet apart. In the DoD, barbed wire is more commonly used as an outrigger than as a standalone fence.

Metal ornamental high security fencing is more aesthetically pleasing than the other fencing types and is one of the most secure types of fencing the DoD uses because it can be equipped with anti-climb inserts, anti-ram cabling, and a K-rated crash barrier, and can house fiber and cabling for other electronic security systems.

3. Considerations

When deciding which type of fencing materials to use for an installation or facility, you must consider:

- The degree of protection required, which would be based on the value of the assets being secured and the threats to those assets
- The cost of the fencing versus the risk

- The location of the fencing, such as whether the fencing will be temporary, as is often used in a tactical environment, or permanent,
- The physical appearance of the fencing. For example, does it need to be aesthetically pleasing and secure, or is security the primary concern?

Lighting

1. Purpose

Lighting serves several purposes in your physical security program. First, lighting deters unauthorized entry. It provides a psychological deterrence to intruders. An intruder may decide the risk of exposure is too great, and therefore, would choose to break in somewhere else.

Second, a properly designed and installed lighting system allows security forces to detect intruders before they reach their targets, or expose them after they reach their targets, depending on the type of lighting in use. When closed-circuit television (CCTV) is used, the lighting system should provide sufficient illumination for the cameras.

Third, the use of glare lighting, which is a type of continuous lighting, can incapacitate intruders by causing discomfort and even disability to an intruder.

For a more detailed look at lighting as a physical security measure, refer to the Exterior Security Lighting eLearning course offered by CDSE.

2. Types

The DoD uses four types of lighting in its installations and facilities. They are:

- Continuous, which consists of a series of fixed luminaries arranged to flood a given area with overlapping cones of light continuously during the hours of darkness
- Standby, which are manually or automatically turned on when suspicious activity is detected or suspected by the security force, alarm system, or motion detector
- Emergency, which is back-up lighting used during power failures or other emergencies when normal systems are inoperative
- Movable, which is normally used to supplement continuous or standby lighting

3. Considerations

When planning what type of lighting to use for the security of your facility, you must consider several factors such as the cost of the lights, characteristics of the lights, positioning of the lights, and maintenance.

a. Characteristics

You must consider the characteristics of different lights when planning which type of lighting to use in a facility. These characteristics include the number of watts required for a given light, the time it takes in minutes for a light to illuminate when

it is first turned on, as well as the time it takes to relight, which is the re-strike time. You must also consider color discrimination and the expected life-span of the particular light. For example, you wouldn't want to use a light fixture that requires frequent light bulb changes in a place that is difficult to reach. Instead, you may want to use a more expensive light bulb that will last longer and require fewer changes.

b. Positioning

A very important factor to consider with your lighting systems is the positioning of the lighting. Light should be directed down and away from the protected area. Every effort should be made to locate lighting units far enough inside the fence and high enough to illuminate areas both inside and outside the boundary. The lights should be located so they avoid throwing a glare into the eyes of the guards but instead create a glare problem for anyone approaching the boundary. In addition, the lights should not create shadowy areas which could identify guard locations.

c. Maintenance

Maintaining light fixtures is very important so the lights are available to keep your facilities secure. Light fixtures must be inspected regularly to replace worn parts, verify that connections are working, repair worn insulation, check for corrosion in weatherproof fixtures, and clean reflecting surfaces and lenses. In addition, the operational hours of lamps should be logged, and the lamps should be replaced between 80 and 90 percent of their rated life.

Man-passable Openings

1. Security Considerations

Virtually every facility and installation has a number of miscellaneous openings that penetrate the perimeter such as drain pipes, sewers, culverts, utility tunnels, exhaust conduits, air intake pipes, manhole covers, air conditioning ducts, fire escapes, equipment access panels, coal chutes, and sidewalk elevators. If any of these openings have a cross-section area of 96 square inches or greater, then a human may be capable of passing through them, hence the term man-passable openings.

Very often these man-passable openings are overlooked in security planning, but they must be taken into account because they are frequently the most effective ways of gaining entrance into a facility without being observed. These openings must be eliminated or at a minimum secured with barriers, grillwork, bars, barbed wire, or doors with adequate locking devices.

Closed Circuit Television

1. Purpose

Closed circuit television (CCTV) plays a very important role in our physical security mission. Using CCTV is an excellent means for deterring 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. Security personnel are able to monitor multiple areas simultaneously, thereby possibly reducing manpower requirements. In some instances, a camera may capture activity missed by security force personnel or details guard force personnel may not be able to readily observe in person.

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 and deter pilferage.

For more information on CCTV, refer to CDSE's Electronic Security Systems eLearning course.

The information in the box below will not be on the test, but it may provide you with useful background and insights.

Closed circuit television is a security system with a camera that captures an image, converts it to a video signal, and transmits it to a monitoring station.

2. Considerations

When considering the use of CCTV as a physical security measure in a facility or installation, you must consider the cost of the system versus the benefit it might provide. Part of the decision includes whether color or black and white is necessary. You must also consider how that system should be protected from tampering and from the elements, if it is installed outdoors. In addition, you must consider if sufficient light is available for the particular model and if light will impact the operation of the cameras.

Intrusion Detection Systems

1. Purpose

An Intrusion Detection System (IDS) is a security system that detects a change in the environment and transmits an alarm, either in the immediate vicinity or to a monitoring station which, in turn, notifies security forces. The purpose of an IDS is to deter, detect, and document intrusion. An IDS does not prevent an intrusion, but rather detects a change in the environment which could be the result of an intruder or something else requiring further investigation.

2. Considerations

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, 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 type and level of criminal activity.

Access Control Systems

1. Purpose and Types

Access control systems allow authorized personnel into a controlled area, such as an installation, building, or controlled space, while preventing unauthorized personnel from entering the area. 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.

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. Employees are trained to recognize and respond to the presence of unauthorized personnel.
- Another form of manual access control is using an acceptable form of identification such as the Common Access Card (CAC).
- Some facilities may still require additional measures for entry which include comparing a valid form of identification to an access roster or the Joint Personnel Adjudication System (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 can be either manual or electronic.

Technology has provided many options in electronic automated access control systems:

- Some employ biometrics, such as fingerprints, hand geometry, handwriting, iris scan, and voice recognition.
- Others, such as card swipe readers, proximity card systems, and key systems do not employ biometrics, but rather, rely on the personal information embedded in the identification card, which is typically the CAC in the DoD.

The information in the box below will not be on the test, but it may provide you with useful background and insights.

A controlled area refers to a facility, installation, or controlled space.

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 Joint Personnel Adjudication System is a system used by host activities to verify the level of access eligibility for visiting individuals.

2. Considerations

The various types of manual and automated access control systems each have various physical security planning and implementation considerations.

One concern with badge systems is the requirement to reissue all badges based upon a percentage of lost or missing badges. Mass reissuance 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. Badge systems also require more security personnel than other manual systems, such as cipher locks, and automated systems.

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. However, there are several things to consider when selecting automated access control systems which range from cost, reliability, and complexity of the technology to file capacity, resistance to counterfeiting, enrollment time, error rates, personal privacy issues, loss of badges, and compromise of PINs. In addition, automated control systems may lead to a false sense of security.

The information in the box below will not be on the test, but it may provide you with useful background and insights.

For card access systems with Personal Identification Number (PIN) options, the readers have keypads into which the PIN is entered. In most cases, the PIN is not stored in the central controller's memory, but is derived from the credential identification (ID) numbers, following some encryption algorithms. In this case, the reader matches the entered PIN with the calculated number to validate the coded credential before it sends the data to the central controller. The preferred method is a system that either assigns a PIN or allows users to select their own PIN that is not related to the badge ID number. PINs are vulnerable to covert discovery by unauthorized personnel via visual observation of the keypad entry sequence or poor control of code numbers by users.

Review Activity 1

Which of the following statements are true about security lighting? Select true or false for each statement. Then check your answers in the Answer Key at the end of this Student Guide.

Statement	True	False
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.	○	○
Certain types of lighting can incapacitate an intruder.	○	○
Controlled lighting is used to illuminate the perimeter of a facility.	○	○

Review Activity 2

Select the appropriate words from the Word Bank to complete the statements below. Then check your answers in the Answer Key at the end of this Student Guide.

Word Bank
A. Barbed wire
B. Concertina wire
C. Chain-link fencing
D. Metal ornamental high-security fencing

1. **[blank]** is often used as a temporary barrier when rolled out on the ground.
2. **[blank]** can be used as permanent standalone fencing but is more often used as an outrigger on the top of the chain link fencing.
3. **[blank]** is more difficult for intruders to scale.
4. **[blank]** is a common type of perimeter fencing for DoD facilities.

Review Activity 3

Which of the following statements are true about physical security measures used in facilities and installations? Select true or false for each statement. Then check your answers in the Answer Key at the end of this Student Guide.

Statement	True	False
Securing man-passable openings is one of the most overlooked physical security protective measures.	○	○
Intrusion Detection Systems (IDS) prevent unauthorized entry.	○	○
Cost and risk must always be considered when planning which physical security measures to use in a facility or installation.	○	○
Access control systems help to prevent unauthorized entry.	○	○
CCTV can deter loss, theft, or misuse of government property and resources.	○	○

Answer Key

Review Activity 1

Which of the following statements are true about security lighting?

Statement	True	False
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.	○	●
Certain types of lighting can incapacitate an intruder.	●	○
Controlled lighting is used to illuminate the perimeter of a facility.	●	○

Review Activity 2

Word Bank
A. Barbed wire
B. Concertina wire
C. Chain-link fencing
D. Metal ornamental high-security fencing

1. **[blank]** is often used as a temporary barrier when rolled out on the ground. *Answer B, Concertina wire.*
2. **[blank]** can be used as permanent standalone fencing but is more often used as an outrigger on the top of the chain link fencing. *Answer A, Barbed wire.*
3. **[blank]** is more difficult for intruders to scale. *Answer D, Metal ornamental high-security fencing.*
4. **[blank]** is a common type of perimeter fencing for DoD facilities. *Answer C, Chain-link fencing.*

Review Activity 3

Which of the following statements are true about physical security measures used in facilities and installations?

Statement	True	False
Securing man-passable openings is one of the most overlooked physical security protective measures.	●	○
Intrusion Detection Systems (IDS) prevent unauthorized entry.	○	●
Cost and risk must always be considered when planning which physical security measures to use in a facility or installation.	●	○
Access control systems help to prevent unauthorized entry.	●	○
CCTV can deter loss, theft, or misuse of government property and resources.	●	○

Student Guide

Course: Physical Security Planning and Implementation

Lesson 4: Physical Security Planning Documents

Lesson Introduction

1. Objective

In order to implement effective protection for DoD assets, documentation of planned physical security measures and procedures is required. These physical security planning documents are as follows: Physical Security Plans, Standard Operating Procedures, Post Orders, Continuity of Operations Plans, and outside agreements called Memorandum of Agreement and Memorandum of Understanding.

Lesson objective:

- Identify physical security planning documents and their purposes, including a facility's Physical Security Plan

Physical Security Plan

1. Purpose

Consistent with DoDI 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB), installation commanders and facility directors must consider threats, assess vulnerabilities, and plan for the protection of assets by clearly defining protective measures required to safeguard DoD assets in a Physical Security Plan. These plans must be constant, practical, flexible to the mission, and responsive to the needs of the installation commander or facility director.

Physical Security Plans for installations and facilities are usually one overarching plan that may be supplemented by local, command, or facility directives, often implemented by Standard Operating Procedures (SOP), and Post Orders. As a physical security professional, you are responsible for recommending the physical security measures to be included in the Physical Security Plan.

2. Parts of the PSP

It is essential that each installation, unit, or activity maintains and uses a detailed Physical Security Plan (PSP). The plan should include the purpose of the plan, the area being secured, the control measures for access and movement and security aids, as well as annexes to the plan, and considerations that must be included when the plan is created for a tactical environment.

The format and specific content of Physical Security Plans may vary between components, installations, units, or activities, but they all cover the same basic information covered in this lesson. Physical Security Plans may contain information that is For Official Use Only (FOUO) or Classified and must be handled accordingly.

a. Purpose

Every Physical Security Plan must include the purpose of the plan. You should state that the plan covers the physical security policies and procedures for the security and safeguarding of a particular area such as an installation or facility and define the area. You should also reference that it covers the assets of any tenant organizations in the installation or facility.

b. Applicability/Area Security

In the Applicability or Area Security section, the plan must outline exactly which areas, buildings, and other structures are covered by the plan.

c. Access and Movement

In the Access and Movement part of the Control Measures section, the plan must outline the controls for personnel, vehicles, and material moving into, out of, and within the installation or facility.

Personnel access controls should include authority for access; what criteria is used for access for different people such as personnel, visitors, maintenance, contractors, and emergency response teams; and identification and control, which should describe the type of system, such as a badging system, that is to be used in each area.

Vehicle access controls should include the policy for conducting searches on military and privately owned vehicles (POVs) parking regulations, and controls for entering into restricted and administrative areas for different types of vehicles such as military and emergency vehicles, and POVs, as well as controls for vehicle registration.

Material controls should include incoming requirements such as search and inspection and special controls on the delivery of supplies into restricted areas, outgoing requirements such as documentation and classified shipments, and controls on the movement of nuclear warheads and chemicals on the installation and in shipments as well as controls for pickups and deliveries of these items.

d. Security Aids

In the Security Aids part of the Control Measures section, the plan must outline how the various physical security measures will be implemented around the installation or facility. These security aids include protective barriers, which include clear zones, signs, and gates; protective and emergency lighting systems; intrusion detection systems (IDS); communications; security forces; contingency plans; use of air surveillance; coordinating instructions with other

military and civil agencies; and physical security measures for the storage of material including storage of materials for all tenants on the installation or facility.

e. Annexes

Annexes to the Physical Security Plan should include, but are not limited to, the following: Threat Statement, Bomb Threat Plan, Installation Closure Plan, Natural-Disaster Plan, Civil Disturbance Plan, Resource Plan, Communication Plan, Designated Restricted/Controlled Areas, Installation Priority Listing, Contingency Plan, and Work-Stoppage Plan.

The information in the box below will not be on the test, but it may provide you with useful background and insights.

Annex A: Threat Statement

The installation threat statement should contain the local threat assessment in relation to the geographic area and attempt to anticipate criminal, terrorist and intelligence activities that threaten installation assets and personnel.

Annex B: Bomb Threat Plan

At a minimum, the bomb threat plan should provide guidance for:

- Control of the operation
- Evacuation
- Search
- Finding the bomb or suspected bomb
- Disposal
- Detonation and damage control
- Control of publicity
- After-action report

Annex C: Installation Closure Plan

At a minimum, the installation closure plan should provide guidance for:

- Road closures
- Restriction plans
- Contingency road closures
- Coordination with local, county and state law enforcement

Annex D: Natural-Disaster Plan

The natural-disaster plan must be coordinated with natural-disaster plans of local jurisdictions. At a minimum, the natural-disaster plan should provide guidance for:

- Control of the operation
- Evacuation
- Communication
- Control of publicity
- After-action report

Annex E: Civil Disturbance Plan

The civil disturbance plan must be formulated by the installation commander or facility director based on local threats. For example, commanders of chemical facilities should anticipate the

need to develop crowd control procedures to handle anti-chemical demonstrations.
Annex F: Resource Plan The resource plan must include the minimum essential physical security needs for the installation or activity.
Annex G: Communication Plan The communication plan is required to establish communications with other federal agencies and local law enforcement agencies to share information about possible threats. The communication plan should address all communication needs for Annexes B through F.
Annex H: Designated Restricted/Controlled Areas This annex must include a listing of all designated restricted/controlled areas on the installation or facility.
Annex I: Installation Priority Listing This annex must include a list of all mission essential vulnerable areas (MEVAs) on the installation or facility.
Annex J: Contingency Plan Contingency plans should include provisions for increasing the physical security measures and procedures based on local commander's assessment of situations of increased threat such as natural disasters or emergencies, or threats from terrorist or criminal elements. Such contingencies may include hostage negotiations, protective services, and special reaction teams. These provisions should be designed for early detection of an attempted intrusion, theft, or interruption of normal security conditions.
Annex K: Work-stoppage Plan A civilian work-stoppage plan may be required for controlling disruptions on an installation or facility.

f. Tactical Environment Considerations

In a tactical environment, the development of a Physical Security Plan is based on METT-TC, which stands for mission, enemy, terrain and weather, troops, time available, and civilian considerations.

- The mission is usually the emplacement of defensive security rings to protect the populace against enemies.
- For enemy, the commander must identify enemy units operating in the area and try to determine the type and size of the unit; the enemy's tactics, weapons, and equipment, and probable collaborators; and the inhabitants' attitudes toward the enemies.
- For terrain and weather, the commander can use observation and fields of fire, cover and concealment, obstacles, key terrain, and avenues of approach (OCOKA) to plan for the physical security defensive sites.
- For troops, the commander must consider available equipment, reaction time, reaction forces, communication assets, organization of troops, and medical support, if available.
- The time available factor is critical since the troops must be ready to respond to an enemy attack with little or no warning.
- For civilian considerations, the commander must consider nonbelligerent third parties such as dislocated civilians, personnel of international businesses and relief organizations, and the media.

The information in the box below will not be on the test, but it may provide you with useful background and insights.

Mission

The following questions must be evaluated:

- What is the mission?
- What specific and implied tasks are there to accomplish the mission?
- What is the commander's intent?

Enemy

The following questions must be evaluated:

- What is known about the enemy?
- Where is the enemy and how strong is he?
- What weapons does the enemy have?
- What is the enemy doing?
- What can the enemy do in response to friendly actions?
- How can we exploit the enemy's weaknesses?

Terrain and weather

The following questions must be evaluated:

- How will the terrain and weather affect the operation?
- How fast can movement be accomplished, and how much space do the terrain and unit formations take up?
- Will the weather affect the terrain or personnel?
- Has the weather already affected the terrain?

Troops

The following questions must be evaluated:

- What are the present conditions of vehicles and personnel?
- What is the status of ammunition and supplies?
- Who is best able to do a specific task?
- How much sleep have the soldiers had in the past 24 hours?
- What other assets are available to support the mission?
- How many teams/squads are available?
- What supplies and equipment are needed?
- What fire support is available and how can it be obtained?

Time available

The following questions must be evaluated:

- How much time is available to conduct planning?
- How long will it take to reach the objective?
- How long will it take to prepare the position?
- How much time do subordinates need?
- How long will it take the enemy to reposition forces?

Civilian considerations

Every commander must prepare a site overlay that shows, at a minimum, the following:

- The attitude of the host nation toward U.S. forces
- The population density near the objective
- The condition of local civilians
- The possible effect of refugees and dislocated civilians on the mission

OCOKA

O – Observation and fields of fire
C – Cover and concealment
O – Obstacles
K – Key terrain
A – Avenues of approach

Other Planning Documents

1. Standard Operating Procedures (SOP)

Standard Operating Procedures (SOPs) provide supplemental guidance for implementing specific components of your physical security program. SOPs are typically established to address operational and administrative physical security procedures to be used during both normal situations, such as key control procedures, access control, and badging procedures, and emergency situations, such as fire, explosions, civil disturbances, major accidents, hostage situations, sabotage, bomb threats, terrorist attacks, and natural disasters. SOPs are specific to an installation or activity; therefore, the quantity and types of SOPs, as well as the contents of each, will vary widely. As a physical security professional, you are responsible for recommending the physical security measures to be included in the Standard Operating Procedures.

The information in the box below will not be on the test, but it may provide you with useful background and insights.

Examples of normal situations:

- Key control procedures
- Access control / badging procedures

Examples of emergency situations:

- Fire
- Explosions
- Civil disturbances
- Major accidents
- Hostage situations
- Sabotage
- Bomb threats
- Terrorist attacks
- Natural disasters

2. Post Orders

Post Orders typically establish duties, roles, and responsibilities at individual assignments, checkpoints, gates, and guard posts. Post Orders allow for uniformity and ensure that everyone involved knows the procedures. Just as with SOPs, Post Orders assist in maintaining order during both normal and emergency situations. At some installations, Post Orders will even be used in a similar manner as or considered one in the same with SOPs. Post Orders may vary among the different components. As a physical security professional, you are responsible for recommending the physical security measures to be included in the Post Orders.

3. Continuity of Operations Plan

In accordance with Executive Order 12656, Assignment of Emergency Preparedness Responsibilities, DoD Directive 3020.26, Defense Continuity Program, directs the DoD to have a comprehensive and effective Defense Continuity Program (DCP) to ensure DoD Component Mission Essential Functions (MEFs) continue under all circumstances across the spectrum of threats.

Heads of the DoD Components develop a Continuity of Operations Plan (COOP) in which they define emergency delegations of authority and orders of succession for key positions; identify and provide for alert notification, movement, and training of continuity staffs; and address information technology and communications support to continuity operations. A COOP typically includes provisions for the complete or partial loss of operational facilities; utilities such as electricity, water, and sewer; telephones and other communications systems; computer systems or computerized components of other systems; and transportation systems.

A COOP is an integral part of the Continuity of Government (COG) and the Enduring Constitutional Government (ECG) under the DCP. It is also a good business practice as it is part of the DoD's functional mission to be a responsible and reliable public institution. As a physical security professional, you have a vital role in identifying security requirements to be considered in the development of this plan including the physical security measures required at alternate work locations used in the event of an emergency.

The information in the box below will not be on the test, but it may provide you with useful background and insights.

Continuity of government (COG) is a coordinated effort within each branch of the government ensuring the capability to continue branch-minimum essential responsibilities in a catastrophic crisis. COG is dependent on effective continuity of operations plans and capabilities.

Continuity of Operations (COOP) is an internal effort within individual DoD Components to ensure uninterrupted, essential DoD Component functions across a wide range of potential emergencies, including localized acts of nature, accidents, and technological and/or attack-related emergencies.

The Defense Continuity Program (DCP) coordinates all defense continuity-related activities and requirements, including Continuity of Operations (COO), Continuity of Government (COO), and Enduring Constitutional Government (ECG).

Enduring Constitutional Government (ECG) is a cooperative effort among the executive, legislative, and judicial branches of the federal government, coordinated by the president, to preserve the capability to execute constitutional responsibilities in a catastrophic crisis. ECG is the overarching goal; its objective is the preservation of the constitutional framework under which the nation is governed. ECG is dependent on effective COOP and COG capabilities.

Mission Essential Functions (MEFs) are the specified or implied tasks required to be performed by, or derived from, statute, Executive Order, or other appropriate guidance, and those organizational activities that must be performed under all circumstances to achieve DoD Component missions or responsibilities in a continuity threat or event. Failure to perform or sustain these functions would significantly affect the Department of Defense's ability to provide vital services or exercise authority, direction, and control.

4. Memorandums of Agreement and Understanding

In certain situations, there exists the need for military installations and facilities to enter into formal agreements with outside activities or agencies to assist in implementing a physical security program. These formal agreements can take the form of a Memorandum of Agreement (MOA) or a Memorandum of Understanding (MOU). Examples of situations that may require an MOA or MOU include provisions for security assistance between DoD activities, either within the same military department or between military departments, or from local law enforcement agencies, and mutual aid from local fire and medical services.

Development of MOAs and MOUs may require coordination at various levels within an activity or organization, but should always include some form of legal review prior to implementation. As a physical security professional, you are responsible for providing guidance and concurrence on the physical security measures to be included in the MOUs and MOAs.

The information in the box below will not be on the test, but it may provide you with useful background and insights.

A Memorandum of Agreement (MOA) or cooperative agreement is a document written between parties to work together on a mutually agreed upon project or to achieve a shared objective. An MOA is a written understanding of the agreement, which may be legally binding but may just be a statement of cooperation between the parties. Sometimes an MOA is interchangeable with a Memorandum of Understanding (MOU). Check with your Component for specific guidance.

A Memorandum of Understanding (MOU) is a document between two or more parties, describing an agreement between those parties. It expresses a shared intention to pursue a common line of action. Unlike a contract, an MOU does not legally obligate the parties, but it is more formal than a gentleman's agreement. Sometimes an MOU is interchangeable with a Memorandum of Agreement (MOA). Check with your Component for specific guidance.

Review Activity 1

Match the physical security planning document to the description that best defines that document's contents; then check your answers in the Answer Key at the end of this Student Guide.

Word Bank
A. COOP
B. MOU/MOA
C. Post Orders
D. SOP
E. PSP

1. Operational/administrative procedures for normal and emergency situations
2. Comprehensive protective measures for an installation, facility, or activity
3. Roles and responsibilities for individual work areas such as checkpoints and guard gates
4. Provisions for back-up facilities, utilities, communication and computer systems, and transportation in the event of a major emergency
5. Provisions for one entity, such as a DoD activity or local law enforcement, fire, and medical services, to provide security assistance to another entity

Answer Key

Review Activity 1

Match the physical security planning document to the description that best defines that document's contents.

Word Bank
A. COOP
B. MOU/MOA
C. Post Orders
D. SOP
E. PSP

1. Operational/administrative procedures for normal and emergency situations. *Answer D, SOP.*
2. Comprehensive protective measures for an installation, facility, or activity. *Answer E, PSP.*
3. Roles and responsibilities for individual work areas such as checkpoints and guard gates. *Answer C, Post Orders.*
4. Provisions for back-up facilities, utilities, communication and computer systems, and transportation in the event of a major emergency. *Answer A, COOP.*
5. Provisions for one entity, such as a DoD activity or local law enforcement, fire, and medical services, to provide security assistance to another entity. *Answer B, MOU/MOA.*

Student Guide

Course: Physical Security Planning and Implementation

Lesson 5: DoD Antiterrorism (AT) Program

Lesson Introduction

1. Objective

In order to combat terrorist activity and protect DoD assets, the DoD has a formal antiterrorism program. This lesson will familiarize you with the tools the DoD uses to protect our nation's assets against terrorist attacks. These tools include DoD Terrorist Threat Levels and Force Protection Conditions (FPCONs).

Lesson objectives:

- Identify what Terrorist Threat Levels are and who establishes them
- Identify what Force Protection Conditions are and who establishes them

AT Program

1. Purpose of the AT Program

Our nation has always been aware of potential terrorist threats. However, incidents such as the attack on the Murrah Federal Building in Oklahoma City in April 1995 and the September 11, 2001 terrorist attacks have proven to us there is a need for increased awareness of the probability of a terrorist attack becoming a reality.

As outlined in DoD Instruction 2000.12, the DoD Antiterrorism (AT) Program is a collective, proactive effort focused on the prevention and detection of terrorist attacks against DoD personnel, their families, facilities, installations, and the infrastructure that is critical to DoD mission accomplishment. The AT Program also provides for the preparation to defend against and planning for the response to the consequences of terrorist incidents. To meet this goal, all DoD employees are required to take annually the Antiterrorism (AT) Level I Training, which is offered by Joint Knowledge Online (JKO).

Additional guidance on antiterrorism is provided in the DoD Antiterrorism Officer Guide, which is For Official Use Only (FOUO) and may not be accessed through this course.

2. AT Tools

Within the DoD Antiterrorism Program, there are AT tools the DoD uses to safeguard DoD assets. Two of these tools are the DoD Terrorist Threat Levels and Force Protection Conditions (FPCONs). Terrorist Threat Levels are analytical assessments of terrorist activity. They are a set of standard terms used to quantify the level of terrorism threat on a country-by-country basis. FPCONs are graduated categories of measures or

actions commanders take to protect personnel and assets from attack. The measures add progressive levels of countermeasures in response to a terrorist threat to U.S. military facilities and personnel.

Threat level assessments, which are based on Terrorist Threat Levels, are provided to senior leaders to assist them in determining the appropriate local FPCONs. However, there is no one for one correlation between Terrorist Threat Levels and FPCONs. For example, a Terrorist Threat Level of Low does not necessarily signify that the local FPCON would be Normal. The FPCON could be ALPHA when the Terrorist Threat Level is Low.

Terrorist Threat Levels

1. Terrorist Threat Levels in the DoD

Terrorist threat levels are based on a continuous intelligence analysis of a minimum of four elements pertaining to terrorist groups: operational capability, intentions, activity, and operational environment. As defined in DoD Instruction 2000.12, DoD Antiterrorism Program, there are four Terrorist Threat Levels: Low, Moderate, Significant, and High.

Defense Intelligence Agency (DIA) or the Combatant Commanders (COCOMs) use Defense Terrorism Warning Reports to convey these Terrorist Threat Levels. The DIA sets the DoD Terrorist Threat Level identifying potential risk to DoD interests in a particular country, regardless of whether U.S. personnel are present in the country. COCOMs with geographic responsibilities may also set Terrorist Threat Levels for specific personnel, family members, units, and installations in countries within their area of responsibility, using the definitions established by the DIA.

2. Threat Levels Defined

DoD Terrorist Threat Levels should not be confused with the Threat Conditions associated with the National Homeland Security Advisory System. DoD Terrorist Threat Levels are identified as Low, Moderate, Significant, and High.

- Low signifies no terrorist group is detected or there is a low risk of terrorist attack.
- Moderate signifies terrorists are present, but there are no indications of terrorist activity and the Operating Environment favors the host nation or the U.S.
- Significant means either that terrorists are present and attacking personnel is their preferred method of operation, or that a terrorist group uses large casualty-producing attacks as their preferred method, but has limited operational activity. The Operating Environment is neutral.
- High signifies terrorists are operationally active and use large casualty-producing attacks as their preferred method of operation. There is a substantial DoD presence, and the Operating Environment favors the terrorist.

As a security professional, it is important to understand the relationship between Terrorist Threat Levels and physical security.

Force Protection Conditions

1. FPCON System

In DoD Instruction 2000.16, DoD Antiterrorism Standards, Force Protection is defined as actions taken to prevent or mitigate hostile actions against DoD assets—including DoD personnel, family members, resources, facilities, and critical information. Force Protection is implemented by establishing Force Protection Conditions (FPCONs).

FPCONs add progressive levels of countermeasures based on the threat. FPCONs are identified as FPCON NORMAL, FPCON ALPHA, FPCON BRAVO, FPCON CHARLIE, and FPCON DELTA. Based on a variety of factors such as terrorist threat analyses and DoD Terrorist Threat Levels, an FPCON is a security posture issued by a Combatant Commander (COCOM). Geographic COCOMs ensure FPCONs are uniformly implemented and disseminated within their area of responsibility. Installation commanders and facility directors, in turn, determine what assets require protection and what FPCON needs to be applied.

The FPCON system allows individuals in authority to be flexible and adaptable in developing and implementing antiterrorism measures that are more stringent than those mandated by higher authorities whenever FPCONs are invoked. Authorities directing implementation may augment their FPCON by adding measures from higher FPCON standards as they deem necessary. Specific physical security measures are outlined for each FPCON in DoDI 2000.16.

2. FPCONs Defined

As you just learned, there are five FPCONs for DoD. They are NORMAL, ALPHA, BRAVO, CHARLIE, and DELTA.

- FPCON NORMAL applies when a general global threat of possible terrorist activity exists and warrants a routine security posture. At a minimum, access control will be conducted at all DoD installations and facilities.
- FPCON ALPHA applies when there is an increased general threat of possible terrorist activity against personnel or facilities, the nature and extent of which are unpredictable. ALPHA measures must be capable of being maintained indefinitely.
- FPCON BRAVO applies when an increased or more predictable threat of terrorist activity exists. Sustaining BRAVO measures for a prolonged period of time may affect operational capability and military-civilian relationships with local authorities.
- FPCON CHARLIE applies when an incident occurs or intelligence is received indicating some form of terrorist action or targeting against personnel or facilities is likely. Prolonged implementation of CHARLIE measures may create hardship and affect the activities of the unit and its personnel.
- FPCON DELTA applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is imminent. This FPCON is usually declared as a localized condition. FPCON DELTA measures are not intended to be sustained for an extended duration.

Review Activity 1

Which of the following statements are true about Terrorist Threat Levels and Force Protection Conditions (FPCONs)? Select true or false for each statement. Then check your answers in the Answer Key at the end of this Student Guide.

Statement	True	False
Combatant Commanders issue both DoD Terrorist Threat Levels and FPCONs.	○	○
Both the DIA and COCOMs issue FPCONs.	○	○
Installation commanders and facility directors issue DoD Terrorist Threat Levels.	○	○
Terrorist Threat Levels are based on information about terrorist groups such as their operational capability and their intentions.	○	○
FPCONs are based on various factors, such as terrorist threat analyses and DoD Terrorist Threat Levels.	○	○

Review Activity 2

Match the term to the description that best defines that term. Then check your answers in the Answer Key at the end of this Student Guide.

Word Bank
A. Terrorist Threat Levels
B. Force Protection
C. DoD AT Program
D. Force Protection Conditions

1. System that standardizes the identification and recommended preventive actions and responses to terrorist threats against U.S. assets
2. The prevention and detection of terrorist attacks against DoD assets as well as the preparation to defend against and planning for the response to the consequences of terrorist incidents
3. Intelligence threat assessments of the level of terrorist threat faced by U.S. personnel and interests
4. Actions taken to prevent or mitigate hostile actions against DoD assets such as DoD personnel, family members, resources, facilities, and critical information

Answer Key

Review Activity 1

Which of the following statements are true about Terrorist Threat Levels and Force Protection Conditions (FPCONs)?

Statement	True	False
Combatant Commanders issue both DoD Terrorist Threat Levels and FPCONs.	●	○
Both the DIA and COCOMs issue FPCONs.	○	●
Installation commanders and facility directors issue DoD Terrorist Threat Levels.	○	●
Terrorist Threat Levels are based on information about terrorist groups such as their operational capability and their intentions.	●	○
FPCONs are based on various factors, such as terrorist threat analyses and DoD Terrorist Threat Levels.	●	○

Review Activity 2

Match the term to the description that best defines that term.

Word Bank
A. Terrorist Threat Levels
B. Force Protection
C. DoD AT Program
D. Force Protection Conditions

1. System that standardizes the identification and recommended preventive actions and responses to terrorist threats against U.S. assets. *Answer D, Force Protection Conditions.*
2. The prevention and detection of terrorist attacks against DoD assets as well as the preparation to defend against and planning for the response to the consequences of terrorist incidents. *Answer C, DoD AT Program.*
3. Intelligence threat assessments of the level of terrorist threat faced by U.S. personnel and interests. *Answer A, Terrorist Threat Levels.*
4. Actions taken to prevent or mitigate hostile actions against DoD assets such as DoD personnel, family members, resources, facilities, and critical information. *Answer B, Force Protection.*

Student Guide

Course: Physical Security Planning and Implementation

Lesson 6: Oversight

Lesson Introduction

1. Objective

Once physical security has been planned for and implemented in an installation or facility, it can only remain effective through oversight of the program. This lesson will familiarize you with the purpose of oversight of security programs and the tools that are used to maintain oversight.

Lesson objective:

- Identify the purpose of oversight and the oversight tools

Oversight Overview

1. Purpose of Oversight

Outlined in DoD 5200.08-R, Physical Security Program, DoD Instruction (DoDI) 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB), the Unified Facilities Criteria, and primarily in individual DoD Component guidance, you will find information about oversight of physical security programs. The purpose of oversight is to ensure that the security program complies with DoD and other policies, that the program is cost-effective, and that the program is effective in protecting DoD assets against threats such as unauthorized disclosure, misuse, damage, and loss. Oversight of all physical security countermeasures such as fencing and barriers, lighting, and other building protective measures must be conducted.

2. Oversight Tools

As you just learned, oversight helps to ensure that DoD physical security programs are properly protecting our assets and are cost-effective. As a physical security professional, you will use several oversight tools to examine how implemented physical security measures are working. These tools include day-to-day observations, surveys, staff assist visits, inspections, and analysis of reports.

Oversight Tools

1. Day-to-Day Observations

The most frequently used oversight tool is day-to-day observations. When you see a security deficiency, such as a security light that has burned out, corrective action must

be taken immediately. Day-to-day observations are an informal method of ensuring that physical security procedures are followed.

2. Surveys

Surveys are a useful way to determine the physical security posture of an installation or facility and to help identify whether an installation or facility has the correct procedures in place to accomplish the mission. Surveys may identify potential vulnerabilities and threats, provide data to prioritize use of physical security resources, provide justification for additional funding, equipment, or manpower, reveal security systems in excess of those required to support the mission, and promote cost effective security, which ensures good stewardship of government resources. Surveys can be informal, which means they are self-initiated within an area, or they can be formal, which means they are directed by installation commanders, facility directors, or higher headquarters.

3. Staff Assist Visits

Staff assist visits (SAVs), also referred to as assist visits or visits, can be extremely useful in determining whether areas of security meet required standards. These visits are conducted to validate the baseline security posture and provide advice on how to meet requirements. They are frequently used when personnel first assume security responsibilities, or as a prelude to the formal inspection process. They are conducted either by peers or by senior agency personnel in the chain-of-command. Assist visits can be broad and of indeterminate scope. Each situation is different and specific to the needs of the individual activity or organization.

4. Inspections

Inspections evaluate and assess the effectiveness and efficiency of the security program. The two types of inspections are management, or self-inspections, and compliance inspections.

a. Management/self-inspections

Management or self-inspections are internal reviews conducted by members of the organization, usually with the aid of a checklist. Some organizations may require self-inspections at regular intervals, such as mid-way through the formal inspection cycle. These inspections serve to aid internal control, prepare for compliance inspections, and ensure that physical security measures are implemented in a cost-effective manner.

b. Compliance inspections

Compliance inspections are formal reviews that evaluate and assess the effectiveness and efficiency of the security program. They are usually conducted by senior officials in the chain-of-command.

Compliance inspections serve a variety of purposes. They identify existing or potential program weaknesses, verify compliance with policies and regulations, promote cost-effective security programs, serve as opportunities for security

education for personnel, promote quality performance of security functions, and establish or enhance good working relationships between security personnel and the various agencies and activities.

The results of a compliance inspection are formally documented with observations, findings, and recommendations. With the inspector's concurrence, discrepancies may be resolved by on-the-spot corrective actions. Inspection reports require timely response and follow-up to correct any deficiencies noted. Inspection results may support requests for increased manpower or other resources necessary to accomplish the security mission.

5. Reports

Incident reports are issued any time a deficiency in a physical security procedure is discovered. These deficiencies may be discovered during informal day-to-day observations or during more formal oversight. Inspection reports are written as a result of an inspection. They contain the findings of the inspection as well as the corrective actions that must be taken.

Conducting Inspections

1. Inspector's Role

Traditionally, inspectors have a reputation of making people nervous and hovering until they find something wrong, but inspectors are really there to help. Their goal is to ensure that DoD resources are protected from threats. To meet this goal, they identify existing or potential weaknesses or security violations and they teach, help, and advise on correct policy and procedures. As a physical security professional, you may at some point be responsible for performing a physical security inspection. Let's take a look at how to conduct an inspection.

2. Pre-Inspection

The most important responsibility an inspector has in preparing for an inspection is to understand the organization, its mission, and its key personnel. The inspector should read any local security directives, the facility's Physical Security Plan, and its Standard Operating Procedures (SOPs), which may implement more stringent policy than higher-level guidance documents. To identify trends and to see what needs to be reviewed for corrections, the inspector should review previous inspection reports. The inspector should also review waivers and exceptions, which give the facility permission to deviate from policy. To manage time and stay focused, the inspector should prepare a plan or checklist and know the scope of the inspection. Finally, the inspector must decide if the inspection should be announced or unannounced. Since one of the goals of an inspector is to create good working relationships, it is usually better to announce the inspection.

3. Beginning the Inspection

When the inspector arrives for the inspection, it is a good idea to meet with the security manager to understand his or her knowledge and perception of the security program and its issues, demands, and needs. This meeting might provide the inspector with

information about areas of focus about which the inspector may not have been aware. The inspector should also conduct an entrance interview with senior management to learn their perspective on their security program and whether they have interest in meeting after the inspection to discuss the inspector's findings. Their answers can indicate to the inspector their level of knowledge and interest in their security program.

4. During the Inspection

During the inspection, the inspector must remember to manage his or her time by using a checklist or plan to follow. The inspector will learn a lot from talking to people who work in the area being inspected. Talking with people will help the inspector to understand what they know and don't know. The inspector should examine and test the products the security manager has in place such as fencing, security lighting, intrusion detection systems, and so on. The inspector should take good notes because these notes will be used to write the inspection report. The inspector should also validate observations as they are made, and look for reasons and causes for security weaknesses or violations. This is a great opportunity for inspectors to teach about policy and changes to policy, as well as advise personnel on new ways to do things, and assist them in getting needed answers and resources.

5. Post-Inspection

After the inspection has been completed, the inspector should brief the security officer or manager on the findings from the inspection and then share findings with senior management, if they requested a meeting about the results. The inspector should not tell senior management anything that was not first told to the security manager. The inspector should include positive observations and not just the shortcomings that were discovered in the inspection. Finally, the inspector should deliver on promises made to the people who were interviewed during the inspection. These promises might include providing follow-up training or phone calls, or providing forms or other resources.

6. Preparing the Inspection Report

When preparing the inspection report, the inspector should think about the purpose of the inspection and whether or not the objectives were met. The report should focus on the objectives and scope that were initially laid out in the inspection plan. The inspector should differentiate between fact and opinion by ensuring that what was seen as a deficiency was truly a policy violation and not just the inspector's opinion of what should be. As with the outgoing meetings with the security manager and senior management, positive observations should be included in the inspection report to support quality performance.

Review Activity 1

Match the oversight tool to the description that best defines that tool. Then check your answers in the Answer Key at the end of this Student Guide.

Word Bank
A. Surveys
B. Staff assist visits
C. Compliance inspections
D. Day-to-day observations
E. Management/self-inspections

1. Internal reviews conducted by members of the organization to aid internal control and ensure cost-effective security program
2. Formal reviews conducted by senior officials in the chain-of-command
3. Validate baseline security posture when personnel assume security responsibilities or as a prelude to a formal inspection
4. Can be self-initiated or directed by higher authorities to determine the physical security posture of an installation or facility
5. Most common and informal oversight tool; immediate action taken to correct deficiencies

Answer Key

Review Activity 1

Match the oversight tool to the description that best defines that tool.

Word Bank
A. Surveys
B. Staff assist visits
C. Compliance inspections
D. Day-to-day observations
E. Management/self-inspections

1. Internal reviews conducted by members of the organization to aid internal control and ensure cost-effective security program. *Answer E, Management/self-inspections.*
2. Formal reviews conducted by senior officials in the chain-of-command. *Answer C, Compliance inspections.*
3. Validate baseline security posture when personnel assume security responsibilities or as a prelude to a formal inspection. *Answer B, Staff assist visits.*
4. Can be self-initiated or directed by higher authorities to determine the physical security posture of an installation or facility. *Answer A, Surveys.*
5. Most common and informal oversight tool; immediate action taken to correct deficiencies. *Answer D, Day-to-day observations.*

Student Guide

Course: Physical Security Planning and Implementation

Lesson 7: Course Conclusion

Course Summary

Planning for the physical security of Department of Defense (DoD) installations and resources is imperative for our national security. You learned about the various components of physical security planning and implementation. These components include physical security roles; the risk management model; physical security planning documents; the DoD Antiterrorism Program, which includes Terrorist Threat Levels and Force Protection Conditions (FPCONs); and the oversight of the physical security program.

Lesson Review

Here is a list of the lessons in the course:

- Course Introduction
- What Is Physical Security Planning and Implementation?
- Facility Design
- Physical Security Planning Documents
- DoD Antiterrorism Program
- Oversight
- Course Conclusion

Course Objectives

You should now be able to:

- ✓ Identify the components of physical security planning and implementation
- ✓ Identify the roles in physical security
- ✓ Identify the components of the risk management model
- ✓ Identify what Terrorist Threat Levels are and who establishes them
- ✓ Identify what Force Protection Conditions are and who establishes them
- ✓ Identify physical security protective measures that should be incorporated into new and existing facility design
- ✓ Identify physical security planning documents and their purposes, including a facility's Physical Security Plan
- ✓ Identify the purpose of oversight and the oversight tools

Conclusion

Congratulations. You have completed the Physical Security Planning and Implementation course. To receive credit for this course, you must take the Physical

Security Planning and Implementation examination. Please use the STEPP system from the Center for Development of Security Excellence to register for the on-line exam.