Student Guide

Course: Introduction to Physical Security

This training course will introduce you to physical security. You'll learn about four main areas: physical security and the roles it involves; security-in-depth; countermeasures; and physical security planning and implementation.

Lesson 1: Physical Security and Roles

Introduction to Physical Security

1. Lesson Introduction

This lesson is about physical security and the roles people play in this continuing effort. The first part of this lesson will provide an overview of physical security policy and history. The second part of this lesson will focus on the roles, responsibilities, and relationships of security professionals in the physical security discipline.

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

- The purpose of physical security
- The history of executive policy documents for physical security
- Department of Defense (DoD) policy documents for physical security
- Roles, responsibilities, and relationships of various command and activity officials relating to physical security

2. Overview

Physical security is defined as that part of security concerned with active, as well as passive measures, designed to prevent unauthorized access to personnel, equipment, installations, materials, and information; and to safeguard them against espionage, sabotage, terrorism, damage, and criminal activity.

Physical security is a major responsibility for installations and facilities. Safeguarding the national security and other Department of Defense, or DoD, assets is not something that is ever taken lightly.

In this lesson, you will learn why we have physical security, how it evolved through the years, how it is mandated throughout the DoD community, and about the various roles, responsibilities, and relationships of security professionals in this continuing effort of physical security.

3. Purpose of Physical Security

The two primary purposes of a physical security program are prevention and protection. Properly designed and executed physical security programs should deter or prevent, to the greatest degree possible, the loss, theft, or damage to an asset.

Our assets are our most critical resources and include personnel, information, equipment, facilities, activities, and operations. Combined, these assets are referred to as PIE-FAO. Deterrents such as guards, signs, dogs, and fences, typically provide sufficient protection against general criminal activity.

Because the United States of America now faces the possibility of terrorist threats like no other time in history, it is paramount that physical security be taken very seriously.

4. History of Executive Policy Documents

Now let's explore the history of executive policies for physical security. Physical security has been around since the beginning of mankind. There has always been a need for the protection of one’s belongings. Through the years, the purpose of physical security has largely remained the same…to protect our assets. However, the methods used in the Physical Security Program have changed significantly.

In December 1952, President Truman signed an Executive Order which provided physical security for facilities deemed important to the national defense mission.

In September 1962, President Kennedy signed an Executive Order prescribing responsibilities of the Office of Emergency Planning in the Executive Office of the President. Essentially, this order made directors of agencies responsible for informing the President of what actions were necessary to physically protect facilities and other assets to national security.

In July 1979, President Jimmy Carter signed an Executive Order to establish the Federal Emergency Management Agency, or FEMA. This agency is charged with planning for national emergencies.

In November 1988, President Ronald Reagan signed an Executive Order that assigned the responsibilities of preparedness for all of the DoD to the Chairman of the Joint Chiefs of Staff, and the responsibility of antiterrorism and force protection to the Secretary of Defense.

On September 11, 2001, the largest attack by terrorists in the U.S. occurred. As a direct result of these terrorist attacks, the U.S. Congress passed, and President Bush signed the Homeland Security Act of 2002, creating the Department of Homeland Security, or DHS.

On October 8, 2001, President George W. Bush signed Executive Order 13228, Establishing the Office of Homeland Security and the Homeland Security Council.

On October 16, 2001, President George W. Bush signed Executive Order 13231, Critical Infrastructure Protection in the Information Age. This order ensures the physical security of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems.

On August 27, 2004, President Bush signed Homeland Security Presidential Directive 12, or HSPD-12, Policy for a Common Identification Standard for Federal Employees and contractors. This requires government-wide development and implementation of a standard for secure and reliable forms of identification for Federal employees and contractors.

In February 2013, President Barack Obama signed Executive Order 13636, Improving Critical Infrastructure Cybersecurity, and Presidential Policy Directive 21, or PPD-21, Critical Infrastructure Security and Resilience.

The policies set forth in these directives are intended to strengthen the security and resilience of critical infrastructure against evolving threats and hazards while also incorporating strong privacy and civil liberties protections into every cybersecurity initiative.

These documents call for an updated and overarching national framework that reflects the increasing role of cybersecurity in securing physical assets.

If you are a history buff, you can use the table below to see how physical security has evolved over the past several years.

Event/E.O.	**Details**
Harry S. Truman **Executive Order 10421** – Providing for the Physical Security of Facilities Important to the National Defense December 31, 1952	

Event/E.O.	Details
John F. Kennedy **Executive Order 11051** – Prescribing Responsibilities of the Office of Emergency Planning in the Executive Office of the President September 27, 1962	(b) The Director, under authority of, and in accordance with the provisions of, Executive Order No. 10421 of December 31, 1952, shall perform functions in respect of the physical security of facilities important to the national defense. (c) In addition, the Director shall review all measures being taken by the Federal agencies with respect to the physical security and protection of facilities important to defense mobilization, defense production, civil defense or the essential civilian economy, including those under the provisions of emergency preparedness assignments to such agencies and shall recommend to the President such actions as are necessary to strengthen such measures.
Jimmy Carter **Executive Order 12148** – Federal Emergency Management July 20, 1979	Executive Order No. 10421, as amended, relating to physical security of defense facilities is further amended by (a) substituting the "Director of the Federal Emergency Management Agency" for "Director of the Office of Emergency Planning" in Sections 1 (a), 1 (c), and 6 (b); and, (b) substituting "Federal Emergency Management Agency" for "Office of Emergency Planning" in Sections 6(b) and 7(b).
Ronald Reagan **Executive Order 12656** – Assignment of Emergency Preparedness Responsibilities November 18, 1988	(a) The policy of the United States is to have sufficient capabilities at all levels of government to meet essential defense and civilian needs during any national security emergency.
June 25, 1996 – **Khobar Towers Bombing**	In 1996, the attack on U.S. forces housed in the Khobar Towers complex in Saudi Arabia, changed attitudes on the protection of U.S. personnel from terrorist attack. As a result of the Downing Commission Report, the Secretary of Defense accepted responsibility for anti-terrorism/force protection (AT/FP) efforts within DoD, and designated the Chairman, Joint Chiefs of Staff (CJCS), as the focal point for all of DoD.
September 11, 2001 – **Terrorist Attacks on the U.S.**	The U.S. Congress passed and President Bush signed the Homeland Security Act of 2002, creating the Department of Homeland Security, representing the largest restructuring of the U.S. government in contemporary history.

Event/E.O.	**Details**
George W. Bush **Executive Order 13228** – Establishing the Office of Homeland Security and the Homeland Security Council October 8, 2001	The functions of the Office shall be to coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States.
Executive Order 13231 – Critical Infrastructure Protection in the Information Age October 16, 2001	Physical Security, co-chaired by the designees of the Secretary of Defense and the Attorney General, to coordinate programs to ensure the physical security of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. The standing committee shall coordinate its work with the Office of Homeland Security and shall work closely with the Physical Security Working Group of the Records Access and Information Security Policy Coordinating Committee to ensure coordination of efforts.
Homeland Security Presidential Directive/HSPD-12 – Policy for a Common Identification Standard for Federal Employees and Contractors August 27, 2004	The Directive requires the development and agency implementation of a mandatory, government-wide standard for secure and reliable forms of identification for Federal employees and contractors.
Barack Obama **Executive Order 13636** – Improving Critical Infrastructure Cybersecurity February 2013 **Presidential Policy Directive 21** – Critical Infrastructure Security and Resilience February 2013	These directives are intended to strengthen the security and resilience of critical infrastructure against evolving threats and hazards while also incorporating strong privacy and civil liberties protections into every cybersecurity initiative. These documents call for an updated and overarching national framework that reflects the increasing role of cybersecurity in securing physical assets.

5. DoD Policy Documents

There are several Department of Defense documents that govern physical security. Let's discuss a few of those.

First there is the DoD Instruction 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB). This document authorizes commanders to issue regulations for the protection or security of property and places under their command. This document also establishes guidelines to build consistent minimum standards for protecting DoD installations and resources.

There is also the DoD 5200.08-R, which is the Physical Security Program regulation. This document implements DoD policies and minimum standards for the physical protection of DoD personnel, installations, operations, and related resources.

Another related DoD regulation is DoDM 5200.01, Volumes 1-4, the Information Security Program regulation. This document addresses the physical security aspects of protecting classified information within the information security program.

There are many other special categories that require physical protection not included in this training. If you are involved in such programs, consult the appropriate guidance.

DoD security is governed by many programs. As a security professional, there may be times that you will need to refer to one of these documents for guidance. You do not need to recall the names and numbers of each of these documents. However, you should be aware of what information is available to guide you in the matters of physical security.

Guidance Document Number	**Guidance Document Title**
DoDM 5100.76	Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives (AA&E)
DoDI 5200.08	Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)
DoD 5200.08-R	Physical Security Program
DoDM 5200.01, Volumes 1-4	DoD Information Security Program
DoDD 5205.07	Special Access Program
DoDS 5210.41-M	Nuclear Weapon Security Manual: DoD Nuclear Weapon Environment-Specific Requirements (U)
DoDI 5210.63	DoD Procedures for Security of Nuclear Reactors and Special Nuclear Materials (SNM)
DoDI 5210.65	Minimum Security Standards for Safeguarding Chemical Agents
DoDI 5210.84	Security of DoD Personnel Assigned to U.S. Missions Abroad
ICD 705	Sensitive Compartmented Information Facilities
DoDI 2000.12	DoD Antiterrorism (AT) Program

6. Summary

So far, you have learned about the primary purpose, history, and Department of Defense policies, regulations, and directives that affect physical security. Physical security covers all of our government's assets, to include personnel, information, equipment, facilities, activities, and operations. The two primary purposes of physical security are prevention and protection. As you proceed throughout this course, you will explore and examine these principles in greater detail.

Review Activity 1

Fill in the blanks by placing each word in the correct sentence. Check your answers in the Answer Key at the end of this Student Guide.

A. People
B. Prevention
C. Protection
D. Operations

___ The two primary purposes of physical security are protection and _______________.

___ ___ The term PIE-FAO, which represents some of our most critical resources, stands for __________, information, equipment, facilities, activities, and ______________.

___ The root purpose of physical security has been the same since the beginning of mankind. That purpose is the ____________ of assets.

Roles, Responsibilities, and Relationships

1. Group Roles

It is important for you to be familiar with the various coordinating activities that play a part in the physical security of DoD assets. These groups include the Antiterrorism Executive Committee, or ATEC, the Antiterrorism Working Group, or ATWG, the Information System Owner, or ISO, the Staff Judge Advocate, and the Threat Working Group, or TWG.

Physical security is not about one entity taking care of everything, but rather several coordinating activities providing an integrated and coherent effort for the protection of national security and other DoD assets. Select each coordinating activity to see the roles, responsibilities, and relationships between these groups.

a. ATWG

ATWG stands for Antiterrorism Working Group. This group is responsible for assessing requirements for physical security, recommending and developing policy, preparing planning documents, and conducting criticality, vulnerability, and risk assessments.

b. ATEC

ATEC stands for Antiterrorism Executive Committee. This executive-level committee should meet at least semi-annually to develop and refine antiterrorism program guidance, policy, and standards and act upon recommendations of the Antiterrorism Working Group and Threat Working Group to determine resource allocation priorities and mitigate or eliminate terrorism-related vulnerabilities.

c. ISO

The Information System Owner, or ISO, is responsible for the security of information systems. This person coordinates physical security measures and develops contingency plans for the protection of the information systems.

d. Staff Judge Advocate

The Staff Judge Advocate works closely with the Antiterrorism Officer and others to ensure that security considerations are properly and legally incorporated.

e. TWG

TWG is also known as the Threat Working Group. This group is comprised of an Antiterrorism Officer, counterintelligence representative, law enforcement representative, operations security officer, information operations representative, and a chemical, biological, radiological, nuclear, and high yield explosive representative.

Commanders of larger installations may choose to include more individuals in their TWG. Local law enforcement agencies can also use their knowledge to assist the TWG.

2. Individual Roles

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, or ATO; Counterintelligence, or CI, support personnel; local, state and Federal law enforcement officials, the Operations Security, or OPSEC, Officer; and the Physical Security Officer.

a. Installation Commander/Facility Director

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

DoDI 5200.08 designates commanders to issue regulations for the protection and security of property or places under their command. In addition, the instruction authorizes the commander to take reasonably necessary and lawful measures to maintain law and order and to protect installation personnel and property.

b. Antiterrorism Officer

The Antiterrorism Officer manages the installation or facility antiterrorism program. This program uses defensive measures to reduce the vulnerability of individuals and property from terrorist attacks. This person is valuable in supporting the physical security mission.

c. CI Support Personnel

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. History has proven that we must always be vigilant.

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, emergency response, and criminal incidents. Coordination activities support mutual understanding of jurisdiction and authority.

e. Operations Security (OPSEC) Officer

The 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 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. They may also coordinate with local law enforcement agencies, antiterrorism officers, and loss prevention personnel.

3. Summary

As you have learned, there are many individuals who play an important part in the mission of physical security. The installation commander, facility director, ATO, Counterintelligence Officer, law enforcement officials, OPSEC Officer, and Physical Security Officer are all links in a chain that is necessary to protect national security and other DoD assets.

Review Activity 2

Fill in the blanks by matching each word on the left to the sentence in which it belongs. Check your answers in the Answer Key at the end of this Student Guide.

A. Law Enforcement
B. Antiterrorism Officer
C. OPSEC Officer
D. CI Support
E. Security Officer

___ _________ is responsible for the installation's antiterrorism program.

___ _________ is responsible for providing valuable information on the capabilities, intentions, and threats of adversaries.

___ _________ analyzes threats to assets and their vulnerabilities.

___ _________ must be integrated into our intelligence gathering process so that they can be part of coordinating emergency responses and criminal incidents on a Federal installation.

___ _________ is charged with management, implementation, and direction of all physical security programs.

Answer Key

Review Activity 1

A. People
B. Prevention
C. Protection
D. Operations

_B_ The two primary purposes of physical security are protection and prevention.

_A_
_D_ The term PIE-FAO, which represents some of our most critical resources, stands for people, information, equipment, facilities, activities, and operations.

_C_ The root purpose of physical security has been the same since the beginning of mankind. That purpose is the protection of assets.

Review Activity 2

A. Law Enforcement
B. Antiterrorism Officer
C. OPSEC Officer
D. CI Support
E. Security Officer

_B_ _________ is responsible for the installation’s antiterrorism program.

_D_ _________ is responsible for providing valuable information on the capabilities, intentions, and threats of adversaries.

_C_ _________ analyzes threats to assets and their vulnerabilities.

_A_ _________ must be integrated into our intelligence gathering process so that they can be part of coordinating emergency responses and criminal incidents on a Federal installation.

_E_ _________ is charged with management, implementation, and direction of all physical security programs.

Student Guide

Course: Introduction to Physical Security

Lesson 2: Security-in-Depth

Security-in-Depth

1. Lesson Introduction

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

Security-in-depth employs security measures in levels or steps. The physical security measures create layers of protection similar to the layers or rings of an onion. Different assets may require different levels of protection. In this lesson, we're going to look at these levels and how they relate to your situation.

Security requirements for classified contracts are stated in DoD 5220.22M, the National Industrial Security Program Operating Manual, or NISPOM. Any additional security requirements levied upon a contractor must be specifically addressed in the contract.

2. Threat, Vulnerabilities, and Criticality

Threat, vulnerabilities, and criticality are essential factors to look at when one is assessing security measures. Let's look at each of these terms and what they mean.

a. Threat

Threat is defined as the perceived imminence of intended aggression by a capable entity to harm a nation, a government, or its instrumentalities, such as intelligence, programs, operations, people, installations, or facilities. A threat can be an indication, circumstance, or event with potential to cause loss of, or damage to, an asset or capability.

We never know when or where a threat may be made to our nation's assets; therefore, it is of the utmost importance that we analyze our vulnerabilities and criticality.

b. Vulnerability

Vulnerability is defined as a situation or circumstance that, if left unchanged, may result in the degradation, loss of life, or damage to mission-essential resources. Vulnerabilities are weaknesses 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, the location of people, equipment, operational practices and even personal behavior.

c. Criticality determination

Criticality determination is based on two things: an asset's importance to national security, and the effect of its partial or complete loss. Look at criticality this way: criticality looks at the importance of a part to the whole. If an asset is necessary to an installation or facility's mission, then that asset has a high level of criticality, and therefore is vulnerable to a threat.

That means we must provide whatever layers of security necessary to protect that asset. Finding this balance will help us to establish what is necessary to protect that asset from a threat.

3. Point vs. Area Security

This section will cover two applications of physical security principles—point security and area security.

a. Point Security

Point security is exactly how it sounds. If you are assigned to point security, you are guarding a specific asset or resource. Two good examples of point security are the crown jewels and the original Constitution of the United States of America. There are guards standing directly in the space of these items, and the jewels and constitution are their respective primary responsibilities. On a military installation or secure Federal building, entry and exit locations are often guarded. This is also an example of point security.

Now that you know what point security means, what do you think area security might mean?

b. Area Security

This type of security is geared towards protecting an entire area of the installation or facility. The goal of area security is to try and consolidate as many assets as possible into one area. This is to intensify the protection efforts while maximizing the effectiveness of response forces. It is important to remember that security professionals employ both point and area security to protect national security and other Department of Defense, or DoD, assets from damage, loss, and theft.

4. Integrating Protective Systems

The protection of national security and other DoD assets is accomplished through the application of active and passive complementary security controls. This integration of physical security measures is also known as security-in-depth. The best way to describe how the integration of physical security measures works is to think of an onion and all the layers it takes to get through to the center. As you begin to peel an onion, it takes more of an effort to reach the center.

Imagine a government facility and add barriers and guard posts with guards in them. Next, imagine a fence around the perimeter along with bright lights and appropriate signs. The government building inside the fence also employs security measures, as there will be guards and security screening equipment one must walk through to get into the building.

Notice the layers of security and how each one is a deterrent. If someone is able to penetrate any of these layers of security, it will take them time and energy to get through to the next layer. That time is what enables our security to defend and defeat before our national security or DoD asset is endangered.

5. Crime Prevention

Crime prevention is a goal. Through awareness, diligence, and the application of active and passive security measures, we can expect to reduce the frequency and severity of crimes against persons and property. We cannot ignore the existence of workplace violence. Just because we work in DoD facilities, this does not make us immune to workplace violence. Crime prevention also includes loss prevention. These crimes adversely affect our organizational resources and our ability to complete missions.

Lesson Summary

Security-in-depth is a concept that employs security measures in levels, or steps. The physical security measures create layers of protection, where different assets may require different levels of protection. Based on the lessons we just learned, you should now have a better understanding of what goes into security-in-depth. Let’s see if we can put it all together.

The criticality of the assets is determined, and then the vulnerability of those assets is evaluated, based on the potential threat. It is important to remember that security professionals employ both point and area security to protect national security and other DoD assets from damage, loss, and theft.

The protection of national security and other DoD assets is accomplished through the application of active and passive complementary security controls. This integration of physical security measures is also known as security-in-depth.

Review Activity

Match each word to the appropriate concept. Check your answers in the Answer Key at the end of this Student Guide.

A. Point Security
B. Onion
C. Criticality
D. Area Security
E. Threat
F. Security-in-Depth

___ Concept that employs security measures in levels or steps

___ Determination based on an asset's importance to national security and effect of loss

___ Security focused on the resource itself

___ Integrated protective systems could be compared to the layers of this

___ The intention and the capability of an adversary to undertake detrimental actions

___ Security is geared towards protecting an entire area of the installation or facility

Answer Key

Review Activity

A. Point Security
B. Onion
C. Criticality
D. Area Security
E. Threat
F. Security-in-Depth

_F_ Concept that employs security measures in levels or steps

_C_ Determination based on an asset's importance to national security and effect of loss

_A_ Security focused on the resource itself

_B_ Integrated protective systems could be compared to the layers of this

_E_ The intention and the capability of an adversary to undertake detrimental actions

_D_ Security is geared towards protecting an entire area of the installation or facility

Student Guide

Course: Introduction to Physical Security

Lesson 3: Countermeasures

Lesson Introduction

Welcome to this lesson on countermeasures. Countermeasures are security measures employed to deter, delay, detect, or prevent adversarial aggression or attacks on identified critical vulnerabilities.

At the end of this lesson, you will have a basic understanding of what countermeasures are put into place to make facilities physically secure. You are going to learn about facility-based protective measures, to include protective barriers and site lighting, security forces, and security systems, and how they play a part in the physical security of an installation. As a security professional, you will need to understand what countermeasures are, and how they play a part in our protection of national security and other DoD assets.

Site Design

1. Overview

Considerable thought goes into designing a secure facility, so it is protected from every angle. The way the site is designed is essential to the protection of mission capabilities, and is necessary for an effective physical security program. Properly designed facilities provide a physical and psychological deterrence to intruders. Poor facility design can also make a facility a possible target for intruders.

Design Consideration	Description
Warning Signs	Warning signs can be easily read by persons approaching on foot or in a vehicle. Restricted area perimeter boundaries shall be posted in conspicuous and appropriate places to clearly identify the area.
Barriers and Fencing	Barriers and fencing are integral parts of all physical security systems. They establish boundaries and deter individuals.
Obstacles	Natural defenses such as waterways, forestations, and ditches, or manmade obstacles such as barricades and vehicle barriers provide for difficult approaches or exit routes.

Design Consideration	Description
Guard Gate	Interior barriers establish boundaries or lines of demarcation of different activities within an installation.
Lighting	Protective lighting should enable guard force personnel to observe activities around or inside an installation without disclosing their presence. Adequate lighting will discourage attempted unauthorized personnel from entering a facility.
Military Dogs	Military working dogs, when properly trained, are intended to supplement and enhance the capabilities of security forces and, therefore, facility protection.

2. Restricted Areas

Restricted areas are areas that require additional protection. Access is limited to authorized personnel. Restricted areas are designated for reasons of security or safeguarding of property or material. It is the responsibility of facility directors or installation commanders to designate restricted areas. By establishing a restricted area, there is improved security due to controlling access, and providing additional layers of security.

Warning signs displaying “Restricted Area” must be posted at the boundary of each restricted area so they can be easily read by persons approaching on foot or in a vehicle. Restricted area perimeter boundaries are posted in conspicuous and appropriate places to clearly identify the restricted area. This includes signs posted at each entrance or logical approach to the area, and or perimeter fences or boundaries of the area that may reasonably be approached by foot or vehicular traffic.

As a security professional you will need to understand what a restricted area is and the importance of providing additional security to certain areas.

3. Building Protective Measures

When considering the physical security of an actual building, several factors come to mind. The number of entrances and exits should always be limited to the minimum necessary for mission accomplishment, as well as for emergency evacuation. Doors are considered a weak spot in a building. They are generally weaker than the building structure, making them less attack-resistant. Windows are also a significant weak point in a building, and are a huge vulnerability. Many roofs of buildings house air conditioners and ventilation systems. They too can be easily exploited if additional measures have not been taken to secure them.

Based on the specific level, value, or sensitivity of information or equipment being protected in a facility, the requirements for construction may be different. When you look closely at all the elements it takes to construct a building, it is easy to see how there could be many vulnerabilities that could allow someone to enter, and possibly access information that could damage our national security or other DoD assets.

Protective measures inside and outside a building all play a role. Walls may be reinforced with steel to make them resistant to attack. Doors may be made of solid steel to resist attack. A protective film covers shatter proof glass and may be used to protect workers inside and keep out potential intruders. Vents are necessary for ventilation. They may, however, be reinforced with steel bars to avert intruders.

4. Summary

Now that we have come to the end of our site design section, let's review what we learned. Restricted areas exist for a reason. It is the responsibility of the facility directors or installation commanders to ensure only authorized personnel are able to access certain areas.

When we are building a house or working in a non-secure building, we take doors, window, roofs and walls for granted; however, when they are all part of a secure environment they are all taken very seriously.

There are many factors to consider when a secure environment is being developed. As a new security professional, it is important for you to understand the importance of every aspect of physical security; however, this is merely an overview of the details that you will learn in the future.

Review Activity 1

Fill in the blanks by placing each word in the correct sentence. Check your answers in the Answer Key at the end of this Student Guide.

A. Controlling Access
B. Requirements
C. Doors

___ The establishment of a restricted area improves security by _______________ and providing additional layers of security.

___ Just by design ______________ are considered a weak spot in the building perimeter, as they are usually weaker than the surrounding building material, and are generally much less attack resistant.

___ Based on the specific level, value, or sensitivity of information or equipment being protected in a given facility, the ____________ for construction may be different.

Protective Barriers

1. Overview

The first line of defense in any physical security system is usually some form of perimeter protection system. The perimeter of an installation or facility is the outermost area of responsibility. Barriers and fencing are an integral part of this protection.

Fencing and barrier devices may be composed of several types of material. Fencing may be chain link fencing, barbed wire fencing, or concertina wire to name a few. Other types of barriers may be poured concrete or hardened steel barriers.

These barriers are also used for establishing boundaries, as well as deterring individuals from attempting unlawful or unauthorized entry. These barriers can also be used as platforms for sensors such as lighting. Barriers also prevent outsiders from being able to view what may be occurring inside the perimeter.

After the terrorist attacks on 9/11, you may have noticed that many barriers suddenly appeared in front of state and Federal buildings. These barriers may have taken up some parking spaces or forced you to walk a longer distance to or from a building; however, as you can now see they were put in place for a reason...to protect personnel and assets of the United States of America from potential terror attacks.

Review Activity 2

Try answering the following question. Select all that apply. Check your answers in the Answer Key at the end of this Student Guide.

1. All of the following are effective protective barriers except:

   □ Steel barriers

   □ Chain link fence

   □ Barbed wire

   □ Human chain

2. Protective barriers are used for all of the following except:

   □ Establishing boundaries

   □ Protecting the facility

   □ Stopping observation

   □ Keeping the facility clean

Site Lighting

1. Overview

Imagine for a moment that you are an intruder who is attempting to gain access to a military installation that serves as the home of the stealth bomber. You have made it past the guard and the entrance over the cement barrier. You are sure you are home free because you just climbed down the barbed wire and you only have one more obstacle between you and the stealth bomber for which you came to take pictures.

You suddenly hear a dog bark and simultaneously you hear a loud click, as a very bright piercing light is glaring in your face. You have no place to run, not only because you cannot see, but also because you have been caught by security forces. As you can see, there are layers of physical security in place for a reason. Site lighting is one of those layers.

Lighting can be used for several purposes. One of those purposes is to enable guard force personnel to observe activities inside or around an installation. Adequate lighting for all approaches to an area not only discourages attempted unauthorized entry, but also reveals persons within a given area. Lighting should supplement other protective measures such as fixed security posts or patrols, fences, and even alarms. There are several varieties of lighting used by DoD installations and facilities including continuous, standby, emergency, and movable lighting.

Type of Lighting	Description
Continuous lighting	Continuous lighting is the most common protective lighting system. It consists of a series of fixed lights arranged to flood an area continuously with overlapping cones of light.
Standby lighting	Standby lighting is similar to continuous lighting, except the lamps are not continuously lighted. They are used when additional lighting is necessary.
Emergency lighting	Emergency lighting depends on alternative power sources and is therefore reserved for times when regular lighting is not available.
Movable lighting	Moveable lighting is used when supplemental lighting is necessary.
Site lighting	Site lighting plays a large part in physical security and countermeasures to protect national security and other DoD assets.

For more information, see CDSE's *Exterior Security Lighting* course.

Review Activity 3

Select True or False for this statement. When you are finished, see the Answer Key at the end of this Student Guide to check your answer.

	True	**False**
Site lighting is used to enable guard force personnel to observe activities inside or outside the installation.	○	○
Standby lighting is used when regular lighting is not available.	○	○

Security Forces

1. Overview

At this point, you have learned that there are several different pieces that make up the countermeasures puzzle. Security forces is the next one you will learn about. Security forces are made up of DoD personnel, military personnel, contract personnel, and even trained dogs, all of which play an active part in protecting our national security and other DoD assets. The majority of installations and facilities maintain a specially identified group of personnel who serve as the enforcement medium for the physical security program.

Typically, the security force is involved in areas such as static observation posts, which guard a high priority resource; access control points that control access to a facility or secure area; roving patrols who ensure the safety and security of the installation or facility to include personnel, information, equipment, and other DoD assets; response forces that respond to the alarms and incidents; security systems monitors who observe alarms and closed circuit television systems; dispatch and control centers that dispatch response forces and mobile patrols and coordinate activities with other personnel; and escorts who are trained personnel responsible for pass and identification, and monitoring individuals.

2. Government and Contract Security

There are typically two types of security force personnel that you will find on a DoD installation or facility. They are government and contract forces. The government security force is made up of Federal government employees who are either military or civilian. Contract security forces are comprised of non-DoD personnel who are employees of a private or commercial source contracted by the Federal government. Whether government or contract, security forces all have the same mission—to protect national security and other DoD assets.

3. Military Working Dogs

Military working dogs, also known as MWD or K-9s, are an integral part of the physical security program. Military working dogs allow security force members to enforce laws and regulations, suppress the use of illegal drugs, detect explosives, and protect DoD installations, facilities, and resources. Military working dogs are capable of performing many duties during law enforcement activities as directed by their handlers. These duties include seek, detect, bite and hold, and guard a suspect. These dogs can also deter attack and defend their handlers during threatening situations.

Military working dogs can also assist in crowd control and confrontation management, as well as search for subjects, both indoors and outdoors. Certain working dogs are even specially trained to detect drugs to assist in providing a drug free environment. Their widely publicized ability to detect drugs makes them a valuable asset to installation commanders. Working dogs are also exceptionally valuable in antiterrorism operations. They can detect unexploded ordnance and search bomb threat scenes. In war fighting roles, military working dog teams provide enhanced patrol and detection capability to perimeter and point defense. Man’s best friend is one of our nation’s most valuable assets in our physical security mission.

4. Summary

By now you have learned there are many pieces to the physical security puzzle, and security forces is just one of them, keeping an installation and its assets safe from potential intrusion. Security forces are made up of contractors, government personnel, and even military working dogs. It takes all of these individuals and groups working together to assist in our physical security efforts. As a security professional, you will need to know the importance of security forces’ roles.

Review Activity 4

Match each type of security force with the statement that best describes the force's roles and responsibilities. Check your answers in the Answer Key at the end of this Student Guide.

A. Government Security Forces

B. Military Working Dogs

C. Contract Security Forces

___ They assist in crowd control and confrontation management, as well as search for suspects both indoors and outdoors. They can detect illegal drugs as well as ordnance.

___ You might see them guarding a gate, monitoring closed circuit monitors or even escorting. They are government employees.

___ They could be manning an entrance or an exit to an installation or they could be sending your bags through an x-ray machine. They work for private contractors employed by the Federal government.

Security Systems

1. Overview

Technology plays an important role in protecting national security and other DoD assets. You are now going to learn about another important protective measure called security systems. In this section you will learn about intrusion detection systems, closed circuit television, access control systems, screening equipment, and two-way radios.

2. Intrusion Detection Systems

An intrusion detection system, or IDS, is an important part of physical security. The purpose of an IDS is to deter, detect, document, and deny or delay intrusion. They detect a change in the environment; this could be the result of an intruder, or something else that may require further investigation.

These detection systems are divided into two types: exterior and interior. Both types of systems are a combination of components, to include sensors, control units, transmission lines, and monitor units, all working together in a specific manner. These systems may seem complicated; however, as a security professional, it is important to understand all aspects of physical security.

a. Exterior IDS

There are a number of different types of exterior sensors in use throughout DoD.

- Fence disturbance sensors do just what their name implies. They detect disturbances of the fence. Invisible barrier protectors detect motion within a specific area, using either microwave or infrared technology.
- A buried line sensor is, in essence, a chain link fence disturbance sensor, buried in the ground. A buried line sensor reacts to vibrations or pressure in a certain area.
- An electric field sensor is composed of multiple wires. One has a current running throughout and the other acts as a sensing mechanism. When something enters the electromagnetic field that is in the wire, the energy in the wire is disturbed and activates an alarm.

b. Interior IDS

Now let’s look at some of the interior intrusion systems.

- Volumetric detectors are designed to detect a change in the environment in a particular area. There are both active and passive volumetric detectors.

- Operable opening switches are used on doors, windows, and other similar openings. They work with either a magnetic switch or a balanced magnetic switch.
- The balanced magnetic switch type should be used in an area requiring high security.
- Interior barrier protectors are used to protect against an amateur intruder. These include an infrared beam or a trip wire.
- Proximity protectors are used to provide point security, and are used to protect items inside a building. They are made up of a capacitance detector and a pressure mat.

3. Closed Circuit Television

Closed Circuit Television, or CCTV, is yet another security measure that can be implemented to provide further protection to national security and other DoD assets. CCTV is simply a closed circuit television system with a camera that captures a visual image, converts it to a video signal and transmits it to a remote location. At the remote location it can be received, displayed, recorded, and printed.

Using CCTV is an excellent means for deterring and detecting loss, theft, or misuse of government property. CCTVs are used in a variety of facilities on any given installation and activity, including commissaries and exchanges, as a means to prevent, deter, and detect pilferage. Security personnel are able to monitor multiple areas simultaneously, thereby saving manpower. CCTV is a reliable and a cost effective tool. It plays a very important role in our physical security mission.

4. Access Control Systems

Access control is a process for ensuring that only authorized personnel are allowed into a designated area. Access controls are implemented to prevent unauthorized personnel from entering designated areas. Access control is one of the inner layers in the overall security-in-depth approach. We learned earlier that physical security is like an onion; it has many layers until you get to the middle, which is the asset to be protected.

The type of access control is determined based on risk management, the process of defining the criticality, vulnerability, and the threat to DoD assets. There are different types of access control systems, from very simplistic manual systems, to more costly automated electronic systems.

One example of a manual system is the non-electronic cipher access control device. This stand-alone system requires only the user to know a 3 or 4 digit number in order to gain access. An example of a manual system that uses automated electronics is the common access card, also referred to as the CAC. The CAC is the size of a credit card, and serves as the standard ID card for DoD. The CAC is used to allow users to authenticate signatures and encrypt e-mails, securely log onto computer systems, and as an access control device into a designated area. When used as primary access control, security personnel must verify the CAC against the person entering the area.

Technology has provided many options in electronic automated access control systems. An example of a basic automated system is the electronic cipher. More complex systems use biometrics. A biometric system uses human individually unique characteristics, such as fingerprints, hand geometry, handwriting, iris scan, and voice recognition. Biometrics is employed to protect particularly sensitive DoD assets. The system used within your area has been selected based on risk management methodologies.

5. Screening Equipment

At DoD installations and facilities, you may encounter guard force personnel using x-ray machines, similar to those seen at airports, scanning hand carried baggage coming into a facility. Additional measures, including portable hand held metal detectors, permanently installed metal detectors, and other specialized equipment may also be used prior to personnel being granted access to those areas.

Certain facilities have always utilized these types of equipment. However, since the terrorist attacks on the Murrah Federal Building in Oklahoma City in April 1995 and 9/11, more facilities have implemented these types of measures in an effort to protect national security and other DoD assets.

6. Two-Way Radio

With any physical security system, communication is key. Two-way radios typically serve as the primary means of communication between response forces and their respective control centers, as well as communication between response force members. While two-way radios are a great tool, there must be backup communications systems available in the event of a catastrophic radio failure. A good Plan B is always necessary!

7. Summary

Now you have learned about yet another layer of the onion that is part of physical security. Security systems that include intrusion detection systems, closed circuit television, access control systems and equipment, and two-way radios are integral in protecting national security and other DoD assets.

For more information, see CDSE’s *Electronic Security Systems* course.

Review Activity 5

Match each type of security system with its definition. Check your answers in the Answer Key at the end of this Student Guide.

A. Two-way radio
B. Intrusion Detection Systems
C. Closed Circuit Televisions (CCTV)
D. Automated access control systems
E. X-ray machines
F. Common Access Card (CAC)

___ This system has a camera that captures a visual image, converts the image to a video signal, and transmits the image to a remote location.

___ This enables individuals to be able to authenticate themselves on secure websites and securely log into computer systems.

___ This system is typically used prior to an individual entering a secure building to ensure they are not entering with any illegal items.

___ This system allows one to be identified by their eye, handprint, or fingerprint.

___ Using these assists in security; however, there must always be back-up communication systems in addition to these.

___ This device sends a signal through wires when it has been triggered.

Facility Access Control Procedures

1. Overview

Facility access control procedures include identification systems, methods of control, and entry and exit inspections, which include search procedures for packages, vehicles, and personal property. Controlling who and what enters a DoD installation or facility is of the utmost importance in our physical security mission.

2. ID Systems and Methods

Will the real John Jones please step forward? Are you who you say you are?

Identification methods are one way of making sure you are who you say you are. This is yet another physical security countermeasure to protect national security and other DoD assets. There are a number of different identification systems being used for access to various areas on an installation or facility. With the advent of Homeland Security Presidential Directive, or HSPD 12, the number of different types of identification media should be reduced, relying heavily on the common identification criteria mandated by HSPD 12. Within the DoD, the Common Access Card is used to fulfill this requirement.

Some facilities, depending on the sensitivity of the area, may still require additional identification methods for entry. Various types of entry control devices may be employed to include personal recognition, automated entry control systems, exchange badge systems, and security personnel conducting physical inspections of identification credentials.

3. Methods of Control

Does that person belong here?

You may see a stranger who does not have the same badge as you, and you may wonder what they are doing in a secure area. It is always a good idea to be aware of your surroundings and the people in your secure area.

There are methods of control to assist with facility access. Through the use of escorts, access control rosters, and in some cases the two-person concept, which requires two people to be present at all times while in a defined area, you should be able to validate those personnel not permanently assigned to an installation or area, who require access to those areas. Whether through a separate badging system identifying visitors, or strict escort rules requiring visitors to be under escort from the time they enter an installation or facility until the time they leave, we must maintain accountability of all visitors.

4. Entry and Exit Inspections

If you have entered a government facility recently, you have more than likely been through the inspection process. You may have had your vehicle searched, either randomly or during a high alert time. You may have had to place your belongings on an x-ray machine or passed through a metal detector to ensure you were not bringing unauthorized items into an area.

Installation and facility authorities determine criteria for conducting inspections of individuals, material in their possession, and vehicles, either randomly or 100%, prior to entering or leaving a controlled area.

- Entry inspections include screening for illegal and prohibited articles such as recording devices, cell phones, or cameras.
- Exit inspections may focus more on unauthorized removal of government assets, including classified information.

This aspect of physical security is important because it serves not only as a great deterrent, but also has value as a means to detect contraband.

5. Summary

As a security professional you will have to understand all aspects of physical security. Facility access control is one more piece to the puzzle. Let’s review what we just covered. There are various identification systems, to include badges, as well as personal recognition and guards doing inspections to name a few. Using escorts for individuals who are not cleared for a certain area assists with limiting access to a need- to-know basis. Inspections and search procedures are inconvenient, but serve a valuable purpose in our effort to protect national security and other DoD assets.

Review Activity 6

Match each type of facility access control with the appropriate description. Check your answers in the Answer Key at the end of this Student Guide.

A. ID check

B. X-ray machine

C. Common Access Card (CAC)

___ Detects unauthorized objects

___ Manual method of control

___ Limits number and types of ID

Lock and Key Systems

1. Overview

We can never have too many layers for protecting national security and other DoD assets. Guards may be employed to provide a level of security for certain areas, and we use security containers to safeguard classified information and other sensitive assets. Now, you will learn how locks and key systems are used for protecting these assets. You are going to learn what locks and keys are authorized for use, as well as how to account for them.

2. Types of Locking Systems

Within the DoD, there are two primary types of locks that you will see being used. These are combination and key-operated locks. The environment and type of asset that is to be protected will usually dictate what type of locking device is selected for use. Consult DoD regulations for specific lock and key requirements.

a. Combination Locks

There are two types of approved combination locks used for the safeguarding of classified information.

The first type is a built-in lock, which may be either the group of locks that meets the FF-L-2740 series federal specification that includes the Kaba Mas X-07, X-08, and X-09, and X-10 locks and the Sargent and Greenleaf, or S&G, 2740 and 2740B locks, or the older style mechanical locks, which met prior standards and in some cases may still be used for classified storage.

The second is combination padlocks that comply with the Underwriter's Laboratory, UL Standard 768-Group 1.

b. Key Operated Locks

There are a number of types of key-operated locks used for other purposes, including low security padlocks and mortise locks.

- Low security padlocks are used to provide limited-to-minimal resistance to forced or surreptitious entry.
- Mortise locks, including deadbolt locks, have a case that is mortised, or recessed, into the frame of the door. Mortise locks are typically found in general office areas and are also considered low security locking devices. Cylindrical locks are the most common type of mortise door lock in use

today. Some cylindrical locks require a key to lock and unlock the door. Others require a key to simply unlock the door.

- The environment and type of asset that is to be protected will usually dictate what type of locking device is selected for use. Consult DoD regulations for specific lock and key requirements.

3. Key Control

Someone once said: An ounce of prevention is worth a pound of cure. For this reason, having a process in place to account for all locks and keys is essential.

Key access and control measures can either be complex or simple, depending upon the program or regulatory requirements. At a minimum, lock and key control procedures should include a key register to list keys, document their issuance, return, and/or disposition. Another control measure would be to have a list of personnel who are authorized access to keys and key records.

When keys are not being controlled and something goes missing, the corrective measures can be very costly, time consuming, and detrimental to the ability to protect DoD assets. As a security professional, you may very well be involved with this process in the future. It is important that you understand the measures it takes to protect DoD assets.

4. Summary

Locks and keys are another means of protecting our classified information. As a security professional, you will undoubtedly have to know what types of locks and keys DoD requires. Let’s review the basics about locks and keys.

Combination and key locks are the two types used on a daily basis within the DoD. The ones used to secure classified information in particular have to meet FF-L-2740 series lock specifications. There are others used for various purposes to include low security padlocks and mortise locks to name a few.

Controlling locks and who has the keys in their possession is also a concern and something that must be taken very seriously to ensure that the keys do not fall into the wrong hands.

Review Activity 7

Match each type of lock with the appropriate description. Check your answers in the Answer Key at the end of this Student Guide.

A. Mechanical combination lock
B. Combination padlock
C. Low security padlock
D. Electromechanical combination lock

___ Complies with FF-L-2740 series lock specification

___ Limited resistance to forced entry

___ Complies with UL Standard 768-Group 1

___ Older style, may be used for classified storage in certain cases

Methods of Storage

1. Overview

You have learned about the many different layers of security it takes to maintain the physical security of a facility. Now we are going to discuss methods of storage; specifically secure rooms, vaults, sensitive compartmented information facilities, and security containers.

2. Secure Rooms, Vaults, and SCIFS

There are several different methods used to secure large volumes of classified information. These include secure rooms, vaults, and sensitive compartmented information facilities, or SCIFs.

a. Secure Rooms

Secure rooms are areas designated and authorized for the open storage of classified information. These facilities are usually built to commercial construction standards, and do not afford the extra security inherent with a “vault.”

b. Vaults

Vaults are constructed to meet strict forcible entry standards. Characteristics that set vaults apart from secure rooms include reinforced concrete on all walls, ceiling, and floor, plus a hardened steel door.

When an area such as a secure room or a vault is approved for open storage, these areas must be constructed in accordance with DoD standards. Other requirements, such as alarms or guard checks, may be required. You should consult your component or agency authority for additional guidance.

c. SCIF

The intelligence community uses a type of storage facility known as a SCIF for the storage of their sensitive compartmented information, or SCI. SCI is derived from intelligence sources, methods, or analytical processes authorized by the Director of National Intelligence.

When building a SCIF, there are strict standards that must be adhered to. These standards address issues such as floors, ceilings, walls, locks, windows, and other openings. For additional information on SCIF construction, refer to ICD 705 IC Tech Spec.

3. GSA-Approved Security Containers

General Services Administration, or GSA, is the authority to approve security containers used to store classified information. Security containers approved for storage of classified information are tested and certified by GSA to ensure that a minimum level of protection against specified methods of unauthorized entry is provided.

These containers must be equipped with locking devices that meet GSA standards. The current standard is FF-L-2740B, which includes the Kaba Mas X-10 and the Sargent & Greenleaf, or S&G, 2740B locks. The Kaba-Mas X-07, X-08, and X-09, and the S&G 2740 locks are still approved for use. Locks that met prior standards were mechanical, and in some cases may still be used for classified storage.

Weapons or sensitive items such as funds, jewels, precious metals, or drugs may not be stored in the same security container used to safeguard classified information. Storage of these items with classified material could increase the risk of compromise to classified information in the security container.

4. Summary

It may seem redundant that after entering a secure facility, one must still be careful with all of the classified materials around them. What we must never forget is that access to classified information is always on a ‘need-to-know’ basis, and there is no reason for anyone to come in contact with something they don’t have an official need-to-know. It is everyone’s responsibility, even within a secure facility, to make sure that classified information does not fall into the hands of someone who could cause damage to our national security.

You now know that classified material must be stored within approved storage containers or facilities. Storage of other sensitive items along with classified information may compromise that classified information.

Review Activity 8

Match each method of storage with the appropriate description. Check your answers in the Answer Key at the end of this Student Guide.

A. SCIF
B. Vaults
C. Secure rooms
D. GSA

___ Areas designed and authorized for the open storage of classified information. These facilities are usually built to commercial construction standards and do not afford the extra security inherent with a vault.

___ Constructed to meet strict forcible entry standards, including reinforced concrete on all walls, ceiling, and floor, plus a hardened steel door.

___ A facility used by the intelligence community

___ The governing authority to approve security containers

Answer Key

Review Activity 1

A. Controlling Access B. Requirements C. Doors	_A_	The establishment of a restricted area improves security by _______________ and providing additional layers of security.
	_C_	Just by design ______________ are considered a weak spot in the building perimeter, as they are usually weaker than the surrounding building material, and are generally much less attack resistant.
	_B_	Based on the specific level, value, or sensitivity of information or equipment being protected in a given facility, the ____________ for construction may be different.

Review Activity 2

1. All of the following are effective protective barriers except:
   - ☐ Steel barriers
   - ☐ Chain link fence
   - ☐ Barbed wire
   - ☒ Human chain

2. Protective barriers are used for all of the following except:
   - ☐ Establishing boundaries
   - ☐ Protecting the facility
   - ☐ Stopping observation
   - ☒ Keeping the facility clean

Review Activity 3

	True	False
Site lighting is used to enable guard force personnel to observe activities inside or outside the installation.	●	○
Standby lighting is used when regular lighting is not available.	○	●

Review Activity 4

A. Government Security Forces
B. Military Working Dogs
C. Contract Security Forces

_B_ They assist in crowd control and confrontation management, as well as search for suspects both indoors and outdoors. They can detect illegal drugs as well as ordnance.

_A_ You might see them guarding a gate, monitoring closed circuit monitors or even escorting. They are government employees.

_C_ They could be manning an entrance or an exit to an installation or they could be sending your bags through an x-ray machine. They work for private contractors employed by the Federal government.

Review Activity 5

A. Two-way radio
B. Intrusion Detection Systems
C. Closed Circuit Televisions (CCTV)
D. Automated access control systems
E. X-ray machines
F. Common Access Card (CAC)

_C_ This system has a camera that captures a visual image, converts the image to a video signal, and transmits the image to a remote location.

_F_ This enables individuals to be able to authenticate themselves on secure websites and securely log into computer systems.

_E_ This system is typically used prior to an individual entering a secure building to ensure they are not entering with any illegal items.

_D_ This system allows one to be identified by their eye, handprint, or fingerprint.

_A_ Using these assists in security; however, there must always be back-up communication systems in addition to these.

_B_ This device sends a signal through wires when it has been triggered.

Review Activity 6

A. ID check
B. X-ray machine
C. Common Access Card (CAC)

_B_ Detects unauthorized objects

_A_ Manual method of control

_C_ Limits number and types of ID

Review Activity 7

A. Mechanical combination lock
B. Combination padlock
C. Low security padlock
D. Electromechanical combination lock

_D_ Complies with FF-L-2740 series lock specification

_C_ Limited resistance to forced entry

_B_ Complies with UL Standard 768-Group 1

_A_ Older style, may be used for classified storage in certain cases

Review Activity 8

A. SCIF
B. Vaults
C. Secure rooms
D. GSA

_C_ Areas designed and authorized for the open storage of classified information. These facilities are usually built to commercial construction standards and do not afford the extra security inherent with a vault.

_B_ Constructed to meet strict forcible entry standards, including reinforced concrete on all walls, ceiling, and floor, plus a hardened steel door.

_A_ A facility used by the intelligence community

_D_ The governing authority to approve security containers

<u>Student Guide</u>

Course: Introduction to Physical Security

Lesson 4: Physical Security Planning and Implementation

Lesson Introduction

Planning for the security defense of an installation or activity must be constant, practical, flexible to the mission, and certainly responsive to the needs of the commander or director. Only through adequate planning can we provide an effective counter response to security threats.

Physical security plans are comprehensive written plans providing for appropriate and economical use of personnel and equipment to prevent or minimize criminal or disruptive activities. In the next few topics, we are going to provide all that you are required to know at this point in your security career about terrorists, antiterrorism, force protection, physical security plans, and inspections and surveys.

Terrorist Threat Levels and Force Protection

1. Overview

In this section, you will learn about terrorist threat levels and force protection conditions. You will learn what terrorist threat levels are, as well as antiterrorism physical security measures, and force protection conditions and responsibilities, also known as FPCON.

Our nation has always been aware of potential terrorist threats; however, incidents such as the Murrah Federal Building in Oklahoma City in April 1995 and the 9/11 terrorist attacks have proven to us there is a need for increased awareness of the probability of a terrorist attack becoming a reality. We must do whatever is necessary in order to protect our national security and other DoD assets.

2. Terrorist Threat Levels

Terrorist threat levels are something many of us are aware of at this time in history. Terrorists are not just an ocean away any longer. Terrorist threat levels should not be confused with Force Protection Conditions, also known as FPCONs. Threat levels are provided to senior leaders in order to assist in determining the appropriate FPCON level. DoD uses a set of standardized terms to quantify terrorist threat levels. Threat levels are identified as Low, Moderate, Significant and High.

a. Low

Low signifies no terrorist group is detected or the terrorist group is non-threatening.

b. Moderate

Moderate signifies terrorists are present but there are no indications of anti-U.S. activity. The Operating Environment favors the Host Nation or the U.S.

c. Significant

Significant signifies anti-U.S. terrorists are present and they attack personnel as their preferred method of operation, or a group uses large casualty-producing attacks as their preferred method, but has limited operational activity. The Operating Environment is neutral.

d. High

High signifies anti-U.S. 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 physical security and terrorist threat levels.

3. Antiterrorism

Antiterrorism is defined as those defensive measures used to reduce the vulnerability of individuals and property to terrorist attacks, to include limited response and containment. Antiterrorism physical security measures integrate facilities, equipment, trained personnel, and procedures into a comprehensive effort designed to provide maximum protection to personnel and other DoD assets.

Well-designed physical security measures include detection, deterrence, delay, denial, and notification. These efforts are accomplished through the development of an antiterrorism plan, outlining who will do what, where, when, and how.

This overview is intended to familiarize you with the basic terminology used in the DoD Antiterrorism Officer, or ATO, Guide. History has proven we must always be vigilant.

4. Force Protection Conditions (FPCONs)

Force Protection is defined as actions taken to prevent or mitigate hostile actions against DoD personnel, including family members, resources, facilities, and critical information.

Force Protection is implemented by establishing Force Protection Conditions, known as FPCONs. FPCONs are a DoD-approved system that standardizes the Department's identification and recommended preventive actions and responses to terrorist threats to U.S. assets. 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.
- 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.
- FPCON BRAVO indicates an increased or more predictable threat of terrorist activity exists.
- FPCON CHARLIE applies when an incident occurs or intelligence is received indicating some form of terrorist action or terrorist targeting against U.S. personnel or DoD assets is likely.
- 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 overview is intended to familiarize you with the basic provisions of the DoD Force Protection Condition System contained in the DoD Antiterrorism Officer, or ATO, Guide.

5. FPCON Responsibilities

Geographic combatant commanders ensure that FPCONs are uniformly implemented and disseminated within their area of responsibility. All installation commanders and facility directors who exercise equivalent authority are responsible for ensuring that their subordinates fully understand the FPCON system.

Individuals in positions of authority need to 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.

6. Summary

Understanding an awareness of world events and the potential effect on the U.S. and DoD assets is critical for decision makers. Let's review what you learned.

Terrorist threat level assessments are provided to senior leaders, who then assign Force Protection Conditions. Once informed, they dictate how the commanders of installations and directors of facilities will prepare and react in implementing their antiterrorism program.

The four DoD threat levels are Low, Moderate, Significant, and High. The five DoD Force Protection Conditions are NORMAL, ALPHA, BRAVO, CHARLIE, and DELTA. For additional antiterrorism training or requirements, consult with your Antiterrorism/Force Protection training source.

Review Activity 1

Match each threat level with its definition. Check your answers in the Answer Key at the end of this Student Guide.

A. High
B. Significant
C. Moderate
D. Low

___ Anti-U.S. 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.

___ No terrorist group is detected or the terrorist group is non-threatening.

___ Anti-U.S. terrorists are present and attack personnel as their preferred method of operation, or a group uses large casualty-producing attacks as their preferred method but has limited operational activity. The operating environment is neutral.

___ Terrorists are present but there are no indications of anti-U.S. activity. The operating environment favors the host nation or the U.S.

Physical Security Plans and Threats

1. Overview

Now you are going to learn about physical security plans, standard operating procedures, or SOPs; post orders, and threat planning. Establishing written plans is essential so everyone involved understands roles, responsibilities, and procedures in the event of an emergency.

2. Physical Security Plans

It is essential that each installation, unit, or activity develop, implement, and maintain a physical security plan. At a minimum, the plan should include special and general guard orders, access and material control, protective barrier and lighting systems, locks, and intrusion detection systems. Physical security plans have the potential to be designated For Official Use Only, or FOUO, or may even be classified, and must be protected accordingly.

3. SOPs and Post Orders

Standard operating procedures, or SOPs, are supplemental guidance for implementing specific components of your physical security program. SOPs are typically established to cover events such as fire, explosion, civil disturbance, major accidents, hostage situations, sabotage, bomb threat plans, terrorism attacks, and natural disaster procedures. SOPs are also implemented to establish operational and administrative physical security procedures such as badging, escorts, and key control. Post Orders typically establish duties, roles, and responsibilities at individual assignments, checkpoints, gates, and guard posts.

SOPs and Post Orders establish duties and responsibilities that allow for uniformity, thereby helping everyone involved know the procedures. Using SOPs and Post Orders will assist in maintaining operational order during both normal and stressful situations.

4. Defining the Threat

Within the physical security program, there are many threats we must consider in the formation of a successful plan. These threats have the potential to cause the loss of or damage to DoD assets or operations. Some examples of threats include criminals, foreign intelligence entities, natural disasters, insiders, and terrorists.

- A criminal is an adversary who commits crimes against people or property such as assault, theft, or hacking into computer systems.

- Foreign intelligence agents are adversaries acting in the interest of a foreign intelligence entity that actively engages in intelligence activities against the U.S. or its assets.
- Natural disasters are natural phenomena that have the potential to damage DoD resources or services or interrupt activities or operations.
- An insider is a trusted person who has been granted access to DoD resources or services. An insider could potentially adversely affect the DoD mission by their criminal behavior.
- A terrorist is an adversary who uses violence or the threat of violence to instill fear with the intent to coerce or intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

5. Summary

Physical security plans are another part of the mission to protect our national security and other DoD assets. When an installation commander or facility director establishes plans for dealing with threats, they improve the security posture, and protect their personnel and assets. Development, implementation, and maintenance of physical security plans, SOPs, and Post Orders will assist in maintaining operational order during both normal and stressful situations.

Review Activity 2

Match each term with the correct description. Check your answers in the Answer Key at the end of this Student Guide.

A. SOPs and Post Orders

B. Physical security plan

C. Threats

___ At a minimum, these should include special and general guard orders, access and material control, protective barrier lighting systems, locks, and Intrusion Detection Systems (IDS).

___ These establish duties and responsibilities which allow for uniformity, thereby helping everyone involved know the procedures.

___ These have the potential to cause the loss of or damage to DoD assets or operations.

Inspections

1. Overview

It would be impossible to manage an effective physical security program without oversight. Inspections are valuable tools to ensure all the necessary steps are being taken to plan accordingly. You are going to learn about the purposes for inspections and types of inspections.

2. Purposes for Inspections

As a security professional, you may be a participant in a physical security inspection, either conducting an inspection, or being inspected. Inspections can verify policy compliance, promote cost effective security, serve as an opportunity for security education, establish and/or enhance good working relationships, identify existing or potential program weaknesses, and promote quality performance of security functions.

As you can see, inspections serve many purposes. The results may be formally documented with observations, findings, and recommendations, or with informal discussions.

3. Types of Inspections

There are two primary types of inspections, compliance inspections and self-inspections.

a. Compliance inspections

The compliance inspection focuses on ensuring regulatory requirements are being met, usually by someone who may be in your immediate chain of command or higher headquarters. Assist visits, command inspections, and Inspector General (IG) inspections are all examples of compliance inspections.

b. Self-inspections

A self-inspection is a review conducted, usually with the aid of a checklist, by members of your own organization. Self-inspections may serve to aid internal control, prepare for compliance inspections, and ensure your physical security program is implemented in a cost effective manner.

4. Summary

Understanding the various types of inspections and their purpose can assist you in preparing for those inspections when the time comes. Let’s quickly review. The purpose of an inspection involves determining compliance with policy, serves as a means of security education, and assists in developing relationships with the organization just to name a few. The types of inspections are compliance and self-inspection.

Review Activity 3

Match each term with the correct description. Check your answers in the Answer Key at the end of this Student Guide.

A. Self-inspection

B. Compliance inspection

___ Can verify that requirements are met, promote cost effective security, and serve as one means of security education. These also establish relationships between the security staff and the organizations population.

___ A review conducted, usually with the aid of a checklist, by members of your own organization. These serve to aid internal control, prepare for compliance inspections, and ensure your physical security program is implemented in a cost effective manner.

Answer Key

Review Activity 1

A. High
B. Significant
C. Moderate
D. Low

_A_ Anti-U.S. 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.

_D_ No terrorist group is detected or the terrorist group is non-threatening.

_B_ Anti-U.S. terrorists are present and attack personnel as their preferred method of operation, or a group uses large casualty-producing attacks as their preferred method but has limited operational activity. The operating environment is neutral.

_C_ Terrorists are present but there are no indications of anti-U.S. activity. The operating environment favors the host nation or the U.S.

Review Activity 2

A. SOPs and Post Orders
B. Physical security plan
C. Threats

_B_ At a minimum, these should include special and general guard orders, access and material control, protective barrier lighting systems, locks, and Intrusion Detection Systems (IDS).

_A_ These establish duties and responsibilities which allow for uniformity, thereby helping everyone involved know the procedures.

_C_ These have the potential to cause the loss of or damage to DoD assets or operations.

Review Activity 3

A. Self-inspection
B. Compliance inspection

_B_ Can verify that requirements are met, promote cost effective security, and serve as one means of security education. These also establish relationships between the security staff and the organizations population.

_A_ A review conducted, usually with the aid of a checklist, by members of your own organization. These serve to aid internal control, prepare for compliance inspections, and ensure your physical security program is implemented in a cost effective manner.