MODULE 13: SECURITY TECHNOLOGY

Day: 6 **Time:** 3.0 Hours **Level of Understanding:** Application

Instructional Strategies:
- Lecture
- Large-Group Discussion
- Video
- Small-Group Exercise
- TeachBack Moment

Module Equipment/Facilities:
- Standard Classroom Setup
- Threaded Exercise Workbook Part 6 — National Ministries Building Answer Key
- National Ministries Building Map

Participant Materials/Handouts:
- Workbook 13.1: PPS Characteristics
- Workbook 13.2: Sensor Types and Characteristics
- Workbook 13.3: Passive Structural Barrier Modifications
- Threaded Exercise Workbook Part 6 — National Ministries Building

Terminal Learning Objective

By the end of this module, you will be able to develop a security technology plan for the protection of critical infrastructure.

Introduction

The third security countermeasure you will be evaluating as part of the physical protection system is technology. Recall from previous modules that a physical protection system is a collection of components designed to work together to achieve protection strategies for a facility. The ultimate objective of the physical protection system is to prevent intruders from accomplishing their desired goals. Many of these technology countermeasure procedures may also apply to cyber security and natural disasters.

Although technology has provided a variety of innovative solutions in meeting those goals, you can apply many low or nontechnology solutions to designing an effective protection system. In this module, you will examine both technical and nontechnical solutions in the areas of detection devices, closed-circuit television monitoring devices, and barrier delay technology. After examining the alternatives available, you will develop a security technology plan for securing a given critical infrastructure providing both high and low technology solutions.

Module Topics

An outline of key topics and an approximate time plan are shown below.

Topic	Enabling Learning Objectives	Approximate Time
Module Introduction	▪ Not Applicable	5 minutes
Characteristics of an Effective Physical Protection System	▪ Describe the characteristics of a physical protection system as they apply to technology.	10 minutes
Primary Physical Protection System Functions — **Detection and Assessment**	▪ Describe the performance characteristics of intrusion detection technology.	45 minutes
Primary Physical Protection System Functions — **Delay**	▪ Explain how nontechnical solutions can be used to delay unwanted intrusion.	30 minutes
Primary Physical Protection System Functions — **Response**	▪ Explain the elements of a security technology plan for protecting critical infrastructure.	20 minutes
Threaded Exercise Workbook Part 6 — National Ministries Building	▪ Develop a security technology plan for protecting critical infrastructure.	60 minutes
Module Summary	▪ Not Applicable	10 minutes

The module times are guidelines only. The actual time required may vary based on the experience level and interest of the participants or other factors encountered during the training session.

Key Terms

Key Term	Description
Active sensor	An electronic device that transmits energy and detects change in the received energy
Balanced protection	A characteristic of an effective physical protection system that ensures no matter how a terrorist intruder attempts to accomplish the attack goal, the intruder will encounter effective elements of the physical protection system
Bistatic microwave sensor	An electronic device composed of two identical microwave antennas installed at opposite ends of the detection zone
Bypassing	The act of going around a sensor's detection zone

Key Term	Description
Contraband detection	Examining personnel, materials, and vehicles to detect unauthorized items using metal detectors, package searches, and explosive detectors
Deployable barrier	An obstacle that is only activated when there is an actual threat or attack
Error rate	The percentage that a specific entry control technique or process falsely rejects an authorized person or falsely accepts an unauthorized person
Flow rate	The measure of the time it takes for an authorized person or material to successfully pass an entry or exit point
Line-of-sight	An expression used to describe a straight line or un-obscured view between two objects
Minimum consequences of component failure	A characteristic of an effective physical protection system that provides contingency plans so that the system can continue to operate even after a component fails
Monostatic microwave sensor	An electronic device composed of a single antenna that is used to both transmit and receive
Passive sensor	An electronic device that detects energy emitted by intruder
Probability of detection	The likelihood that an intrusion detection system senses and actual threat or attack
Protection-in-depth	A characteristic of an effective physical protection system that requires an intruder to avoid or defeat a number of protective devices in sequence to reach an objective or target
Seismic sensor	A device that detects vibrations in the ground, most often used to detect the magnitude of earthquakes
Spoofing	The act of passing through a sensor's normal detection zone without triggering the alarm
Type I error	The false rejection of an authorized person
Type II error	The false acceptance of an unauthorized person

Abbreviations/Acronyms

Abbreviation/Acronym	Description
kHz	Kilohertz

This Page Intentionally Left Blank.

Topic: Module Introduction — 5 Minutes

Slide 1 Security Technology

- Title Slide

Graphic Description: US Flag and Seal

Module Preparation

- **Timing and Methods:** Use the suggested time plan at the beginning of the module. As with all modules in this course, read all the content (Facilitator Guide and PowerPoint slides) and familiarize yourself with each facilitator note before class.
- Be thoroughly prepared for exercises, discussions, or other activities required for the module. Follow all facilitator notes. Use a combination of lecture, large-group discussion, small-group activities, and TeachBack moments.
- Note: be prepared to discuss technological security countermeasures of the host facility whether it is identified as a critical infrastructure or not.

Orientation to Participant Guide

- When beginning this module:
  - Refer participants to the beginning of this module in the Participant Guide.
  - Note the list of addendums participants will use during this module. Explain that instructions for all exercises are included in the addendums.
  - Review the key terms and abbreviations/acronyms before beginning the module.

Slide 2 Module Objective

- By the end of this module, you will be able to develop a security technology plan for the protection of critical infrastructure

Graphic Description: No Graphic

- Briefly discuss the terminal learning objective.
- Highlight the key topics to be presented:
  - Characteristics of a Physical Protection System
  - Primary Physical Protection System Functions — Detection and Assessment
  - Primary Physical Protection System Functions — Delay
  - Primary Physical Protection System Functions — Response
- Ask participants whether they have any questions about anything covered thus far.

Slide 3 PPS Diagram

- *No Text*

Graphic Description: Physical protection system diagram with Identify Security Countermeasures box highlighted in yellow

- Show the participants where this module is in relation to the PPS Diagram.
- Review the three security countermeasures involved in this phase:
  - Policies and procedures were covered in *Module 11: Policies and Procedures*.
  - Security force was covered in *Module 12: Security Force Operations*.
  - Technology will be covered in this module.
- Explain that once security countermeasures have been identified they must be inspected and validated.
- Tell participants that security inspection and validation involves establishing evaluation criteria for the three security countermeasures listed above and will be covered in *Module 14: Security Inspection and Validation*.
- Refer to the physical protection system diagram to see a visual representation of the relationship between the three security countermeasures listed above.

Topic: Characteristics of a Physical Protection System — 10 Minutes

Enabling Learning Objective:

- Describe the characteristics of a physical protection system as they apply to technology.

Slide 4 Characteristics of a Physical Protection System (Workbook 13.1)

- Protection-in-depth
- Minimum consequences of component failure
- Balanced protection

Graphic Description: Security force approaching a flimsy door in a brick wall

- Refer participants to **Workbook 13.1: PPS Characteristics**.
- Remind participants that in *Module 12: Security Force Operations* they were introduced to the three primary physical protection system functions: detection and assessment, delay, and response.
- Emphasize that these three functions create the foundation for an effective physical protection system, along with the three characteristics listed on the slides.
- Define the following terms:
  - **Protection-in-depth:** a characteristic of a physical protection system that requires an intruder to avoid or defeat a number of protective devices in sequence to reach an objective or target.
  - **Minimum consequences of component failure:** a characteristic of a physical protection system that provides contingency plans so that the system can continue to operate even after a component fails.
  - **Balanced protection:** a characteristic of a physical protection system that ensures no matter how a terrorist intruder attempts to accomplish the attack goal, the intruder will encounter effective elements of the physical protection system.

- Using the addendum briefly discuss each of these characteristics.
- Explain the reasons that completely balanced protection is not only impossible, but also undesirable.

Topic: Primary Physical Protection System Functions — Detection and Assessment	**45 Minutes**

Enabling Learning Objective:
- Describe the performance characteristics of intrusion detection technology.

Slide 5 Primary Physical Protection System Functions — Detection and Assessment

- *No Text*

Graphic Description: Primary physical protection system functions diagram with Detection and Assessment box highlighted in yellow

- Refer participants to the figure on the slide.
- Emphasize that the three primary functions of a physical protection system are interrelated and complementary of one another; however, their individual complexity requires individual examination of each function.
- Point out the Detection and Assessment function (highlighted in yellow).
- Remind participants that the response function was covered in detail in *Module 12: Security Force Operations*, therefore, only a very brief review of the response function will be provided.
- Tell participants the four elements of detection will be covered in the upcoming subsections, starting with intrusion sensing.

Slide 6 Intrusion Detection Systems (1 of 2)

- Designed to detect unauthorized persons or vehicles attempting to gain access to a protected critical asset
- Intended to supplement security forces, **not** replace them

Graphic Description: No Graphic

- Define **intrusion detection system:** a combination of physical, electronic, and computer methods used to detect unauthorized persons or vehicles attempting to gain access to a protected critical asset.
- Remind participants that *Module 2: Introduction to Critical Infrastructure Security and Resilience* defined detection as the discovery of a terrorist action that includes sensing covert (hidden) or overt (obvious) actions.
  - Detection is not an instantaneous event, but a process involving assessment.
  - To effectively discover an action, the following elements are present:

    - A sensor reacts to a stimulus and initiates an alarm.
    - Information from the sensor and assessment subsystems is reported and displayed.
    - A person assesses the information and determines if the alarm is valid or invalid.
- Explain that an intrusion detection system supplements the existing security force, enhancing their ability to react to attempted or real intrusions.
    - An intrusion detection system is not a substitute for a security force.
    - If an intrusion detection system were to replace the security force, there would be no one to acknowledge the alarm, assess it, or respond to it.
- Remind participants of the definition of intrusion detection system used in the context of cybersecurity in *Module 7: Cybersecurity*: software that automates the intrusion detection process; may or may not be detectible to the intruder.

Slide 7 Intrusion Detection Systems (2 of 2)

- Consist of the following components working together to create an intrusion detection boundary:
    - Exterior and interior intrusion sensors
    - Video alarm assessment
    - Entry control and alarm communication

Graphic Description: Electronic entry control devices in restricted area

- Explain that the intrusion detection boundary created by an intrusion detection system helps ensure that all intrusion, whether by surface, air, underwater, or underground are detected.
- Explain the components of intrusion detection systems.
    - **Exterior and interior intrusion sensors** — operate in the outdoor environment and inside buildings
    - **Video alarm assessment** — without personnel to acknowledge, assess, and respond to an alarm, an intrusion detection system would be ineffective
    - **Entry control and alarm communication**:
        - Allows entry to authorized personnel.
        - Detects the attempted entry of unauthorized personnel and material.
- Tell participants that performance characteristics of intrusion detection are presented in the next slides.

Slide 8 Performance Characteristics

- This section will cover:
    - Probability of detection
    - Vulnerabilities to defeat

Graphic Description: No Graphic

- Explain that intrusion sensing performance can be described by several characteristics; each characteristic will be covered in the upcoming subsections, starting with probability of detection.

Slide 9 Probability of Detection (1 of 2)
▪ The likelihood that an intrusion detection system senses an actual threat or attack ▪ The design of the physical protection system should specify the detection criteria required or expected of a sensor or sensor system
Graphic Description: No Graphic

Slide 10 Probability of Detection (2 of 2)
▪ Factors that may influence the probability of detection for a specific sensor: • Target to be detected • Sensor hardware design • Installation conditions • Sensitivity adjustment • Weather conditions • Condition of the equipment
Graphic Description: Electronic light and movement sensor

- Define **probability of detection:** the likelihood that an intrusion detection system senses an actual threat or attack.
- Provide examples from facilitator experience of the factors that influence detection:
  - Target to be detected
  - Sensor hardware design
  - Installation conditions
  - Sensitivity adjustment
  - Weather conditions
  - Condition of the equipment
- Emphasize the fact that no sensor is perfect and that probability of detection is conditional, based on assumptions made about the conditions in which the sensor operates.
- Do not explain the mathematical equations involved in determining probability of detection.

Slide 11 Vulnerabilities to Defeat
▪ **Bypassing** — going around a sensor's detection zone ▪ **Spoofing** — passing through a sensor's normal detection zone without triggering the alarm
Graphic Description: No Graphic

- Tell participants that an intrusion detection system can be vulnerable to defeat in several ways.
- Define the following terms:
  - **Bypassing:** the act of going around a sensor's detection zone.

- **Spoofing:** the act of passing through a sensor's normal detection zone without triggering the alarm.

Slide 12 Discussion Question
▪ Drawing from your own experiences, what are some examples of bypassing and spoofing?
Graphic Description: No Graphic

- Ask participants: **Drawing from your own experiences, what are some examples of bypassing and spoofing?**
- Acknowledge responses. *Responses will vary.*
- Ask participants whether they have questions on intrusion sensing performance characteristics or anything else covered thus far.

Slide 13 Intrusion Sensor Application (Workbook 13.2) 
▪ Must determine how sensors should be used in the protected area ▪ Application modes are different for exterior sensors and interior sensors ▪ Classified as: • Passive or active • Covert or visible
Graphic Description: No Graphic

- Refer participants to **Workbook 13.2: Sensor Types and Characteristics.**
- Tell participants they may use the addendum as a reference to follow along.
- Explain that how sensors are used — their application — is different depending on whether the protected areas are exterior or interior.
- Explain that passive sensors:
  - Detect some type of energy that is emitted by the intruder.
  - Detect the change of some natural field of energy caused by the target, such as the change in the local magnetic field caused by the presence of metal.
  - Use a receiver to collect energy emissions.
  - Include sensors based on vibration, heat, sound, and electrical currents (capacitance).
  - For example, a passive sensor can detect mechanical energy emitted from a person walking on the soil or climbing on a fence.
- Explain that active sensors:
  - Transmit various types of energy.
  - Detect a change in the received energy created by the presence or motion of the target.
  - Include both a transmitter and a receiver and include microwave, infrared, and radio frequency devices.
  - For example, correctional (prison) facilities often incorporate active sensors in the design of their perimeter fences to detect escaping prisoners before they reach the last fence to freedom.

- Tell participants that passive and active sensors can be used for both interior and exterior security system design.
- Explain the distinction between the use of passive and active sensors.
  - The presence or location of a passive sensor is more difficult to determine than that of an active sensor since there is no energy source to locate — this puts the intruder at a disadvantage.
  - In environments with explosive vapors or materials, passive sensors are safer than active ones because no energy is emitted that might initiate explosives.
  - Active sensors more effectively reduce nuisance alarms because of their stronger signals.
- Emphasize the distinction between covert and visible sensors.
  - Covert sensors are hidden from view, such as sensors buried underground; since they are more difficult for an intruder to detect and locate, covert sensors can be more effective.
  - Visible sensors are in plain view, such as sensors attached to a fence or mounted on a support structure, and that visibility may deter an intruder from acting; these sensors are usually easier to install, repair, and maintain than covert sensors.

Slide 14 Discussion Questions (1 of 2) (Workbook 13.2)

- How can pressure or **seismic sensors** be defeated?
- How can magnetic field sensors be defeated?
- How can ported coaxial cable sensors be defeated?
- How can fiber-optic cable sensors be defeated?

Graphic Description: No Graphic

- Define **seismic sensor**: a device that detects vibrations in the ground, most often used to detect the magnitude of earthquakes.
- Ask participants:
  - **How can pressure or seismic sensors be defeated?**
  - Acknowledge responses. *Answers may vary but should include: form a low bridge over the transducer line, and use precision parachute jumps (creative and uncommon approach).*
  - **How can magnetic field sensors be defeated?**
  - Acknowledge responses. *Answers may vary but should include: avoid wearing or carrying metal.*
  - **How can ported coaxial cable sensors be defeated?**
  - Acknowledge responses. *Answers may vary but should include: wooden stilts, pole vaulting, bridging, salt leaching, and locate and cut the cable.*
  - **How can fiber-optic cable sensors be defeated?**
  - Acknowledge responses. *Answers may vary but should include: locate and cut the fiber-optic cable.*

Slide 15 Discussion Questions (2 of 2) (Workbook 13.2)

- How can fence-disturbance sensors be defeated?
- How can sensor fences be defeated?
- How can a sensor fence be designed to deter tunneling (digging under)?

Graphic Description: No Graphic

- **How can fence-disturbance sensors be defeated?**
- Acknowledge responses. *Answers may vary but should include: digging under or bridging over the fence without touching the fence itself.*
- **How can sensor fences be defeated?**
- Acknowledge responses. *Answers may vary but should include: tunneling, pole vaulting, bridging, and clamping and cutting wires.*
- **How can a sensor fence be designed to deter tunneling (digging under)?**
- Acknowledge responses. *Answers may vary but should include: putting concrete under the fence and placing the bottom edge of the fence fabric in the concrete.*

Slide 16 Application Modes for Exterior Sensors (Workbook 13.2)

- *Video*

Graphic Description: Video of an intruder first running in shadows and then crawling in shadows to avoid detection

- Emphasize the characteristics of video motion detectors as identified in **Table 1: Exterior Sensors** of **Addendum 13.2: Sensor Types and Characteristics**.
- Click on the arrow below image to play the video.
- Explain that it illustrates how an intruder can defeat sensor detection by running and crawling in shadows.
- Emphasize that improper camera placement and poor lighting contribute to inferior visibility.
- Remind participants that periodic reviews of the closed-circuit videos were discussed in *Module 11: Policies and Procedures*.
- Ask participants whether they have questions on exterior sensor application modes or anything else covered thus far.

Slide 17 Application Modes for Interior Sensors (Workbook 13.2)

- Boundary-penetration sensors
- Interior motion sensors
- Proximity sensors

Graphic Description: Interior motion sensor (top); proximity sensor under a tarp and a mat (bottom)

- Explain the types of sensors shown on the slide:
  - **Boundary-penetration sensors** — detect an intruder crossing the boundary from an exterior to an interior area.

  - **Interior motion sensors** — detect the movement of an intruder within a confined interior area.
  - **Proximity sensors** — detect intrusion in the area immediately adjacent to an object or when a specific object is touched.
- Refer participants to **Table 2: Interior Sensors** in **Workbook 13.2: Sensor Types and Characteristics**.
- Explain the characteristics of each interior sensor type listed.
- Remind participants that active infrared sensors were covered in the exterior sensor section; these are active, visible, and line detection sensors.
- Explain that interior active infrared uses infrared beams (invisible to the human eye), configured into a vertical infrared fence.

Slide 18 Discussion Questions (1 of 2) (Workbook 13.2)

- How can vibration sensors be defeated?
- How can electromechanical sensors be defeated?
- How can interior active infrared sensors be defeated?

Graphic Description: No Graphic

- Ask participants:
  - **How can vibration sensors be defeated?**
  - Acknowledge responses. *Answers may vary but should include: if the vibration sensitivity level is known to be low, an intruder can use a glasscutter to cut through the window.*
  - **How can electromechanical sensors be defeated?**
  - Acknowledge responses. *Answers may vary but should include: use a jumper cable around a cut (circumventing the sensor by providing electrical continuity through the jumper cable), and removing both the switch unit and the magnetic unit together, keeping the magnetic field between the two intact.*
  - **How can interior active infrared sensors be defeated?**
  - Acknowledge responses. *Answers may vary but should include:*
    - *Bridging*
    - *Beam capture*
    - *Step or slide through the beams*

Slide 19 Discussion Questions (2 of 2) (Workbook 13.2)

- How can monostatic microwave sensors be defeated?
- How can video motion detector sensors be defeated?
- How can you defeat pressure sensors?

Graphic Description: No Graphic

  - **How can monostatic microwave sensors be defeated?**
  - Acknowledge responses. *Answers may vary but should include:*
    - *Crawling through the offset zones (zone of no detection, which exists in the first few meters in front of the antenna).*

    - *Tunneling under.*
    - *Bridging over (if bridging equipment is high enough).*
  - **How can video motion detector sensors be defeated?**
  - Acknowledge responses. *Answers may vary but should include: intruder wearing clothing similar to observation area, intrusion during times of obscured vision or low lighting, or camouflaging the target in the background.*
  - **How can you defeat pressure sensors?**
  - Acknowledge responses. *Answers may vary but should include: stepping around or bridging over the mat.*
- Ask participants whether they have any questions on interior sensor application modes or anything else covered this far.

Slide 20 Alarm Communication and Display Systems (1 of 2)
▪ Provide security personnel with rapid response capability ▪ Perform two critical tasks: • Transport alarm and assessment information to a central point • Provide information to the security control center operator
Graphic Description: Many monitors of an alarm display system

- Explain the two critical tasks of an alarm communication and display system.
  - Transport alarm and assessment information to a central point
  - Provide information to the security control center operator — once the operator receives the information, the alarm communication and display system also make it possible for the operator to enter commands to control the system.

Slide 21 Alarm Communication and Display Systems (2 of 2)
▪ Five subsystems: • Communications • Line supervisions and security • Information handling • Control display and alarm assessment • Off-line functions ▪ Subsystems enable operators to respond appropriately
Graphic Description: Emergency communication phone in a parking garage

- Tell participants that alarm communication and display systems are divided into five subsystems:
  - **Communications** — transfers data from the collection point (sensors) to a security control center.
  - **Line supervision and security —** network layer of the system that monitors any errors or disruptions in communication transmission.
  - **Information handling —** when alarm data is transmitted from the sensors to a security control center (may be a single computer or multiple computers); the security control center processes the alarm data into useful information.

- **Control display and alarm assessment —** equipment and processes to:
  - Determine alarm status (malfunctioning, disabled, or breached)
  - Conduct alarm assessment and enter appropriate response commands
- **Off-line functions —** performs noncritical functions, such as:
  - Event logs
  - Databases
  - Event printers

- Explain that when these subsystems are fully integrated, effective transmission of alarm data enables the operator to respond appropriately.

Slide 22 Alarm Communication and Display System Characteristics
▪ Fast reporting time ▪ Secure from attack ▪ Durable ▪ Backup capable ▪ User friendly
Graphic Description: Exterior security cameras; compact disks for data storage

- Explain that an alarm communication and display system has certain characteristics that contribute to overall effectiveness.
  - **Fast reporting time —** the single most important measure of alarm communication and display effectiveness is how well it quickly and clearly communicates the following alarm data from sensors to the system operator:
    - Where an alarm has occurred.
    - What or who caused the alarm.
    - When the alarm happened.
  - **Secure from attack:**
    - Because the physical protection system protects a critical infrastructure's most important assets, it is reasonable to assume that the alarm communication and display system must be secure from attack.
    - For example, procedures should limit who has access so that only authorized persons should have access to alarm communication and display information, components, and wiring.
  - **Durable:**
    - If a component will be subject to wide temperature variations (such as in an exterior environment), the equipment must be designed to withstand the variations without failing.
    - The individual components should be reliable and break down infrequently (a long average time between failures).
    - A reliable system requires maintenance and operators trust the system.
    - Other aspects of reliability include dependable communication and display of alarm data and no loss of information
  - **Backup capable —** effective alarm communication and display systems take the chance of failure into account and establish backup capability for critical components.

  - **User-friendly:**
    - Alarm communication and display systems must be easy to operate.
    - While multiple sensors can provide considerable information, this data must be displayed in a manner that presents the critical information to the operator.
    - A system that is easy to use also reduces training time and retraining needs.
- Ask participants whether they have any questions on alarm communication and display or anything else covered thus far.

Slide 23 Alarm Assessment
▪ Purpose: • Determines the cause of an alarm • Provides additional information for security force ▪ Provided through: • Closed-circuit television coverage of each zone • Visual checks by personnel ▪ Closed-circuit television may provide assessment and surveillance
Graphic Description: No Graphic

- Remind participants that a fundamental principle of physical protection system design is detection is not complete without assessment.
- Explain the two purposes of alarm assessment:
  - Determines the cause of an alarm — whether the alarm is due to an intruder or a nuisance.
  - Provides additional information about an intrusion to the security force team to assist in making response decisions.
- Explain the two ways alarm assessment can be provided:
  - Closed-circuit television coverage of each zone — authorized personnel can quickly assess sensor alarms at remote locations and avoid unnecessary deployment of security force members to an area.
  - Visual checks by personnel.
- Emphasize that since this module focuses on technology, the next section will address alarm assessment through use of closed-circuit television cameras.
- Distinguish the difference between assessment and surveillance with respect to closed-circuit television:
  - Closed-circuit television can be used for both assessment and surveillance.
  - **Assessment:**
    - Refers to the use of closed-circuit television to capture images of a sensor detection zone immediately at the time of an intrusion alarm.
    - Another term for the detection zone is assessment zone.
    - The images can then be reviewed to determine the cause of the alarm and the proper response can be initiated.
  - **Surveillance:**
    - Uses closed-circuit television to monitor activity in the area continually, without the benefit of intrusion sensing.

    - Many surveillance systems do not even include human operators — they simply record activity periodically on videotape for later review.
- For the purposes of this module, the section to follow is based on the premise that assessment will be accomplished by using closed-circuit television cameras.

Slide 24 Discussion Question
▪ When would security force members need to perform an alarm assessment?
Graphic Description: No Graphic

- Ask participants: **When would security force members need to perform an alarm assessment?**
- Acknowledge responses. *If not provided by participants, add the following: when the video alarm assessment system is:*
    - *Inoperable (due to weather).*
    - *Unavailable (due to maintenance).*

Slide 25 Alarm Assessment Components (1 of 3)
▪ Camera, lens, and mount ▪ Lighting system ▪ Video transmission system ▪ Video switching equipment ▪ Recorder, monitor, and controller
Graphic Description: No Graphic

- Tell participants alarm assessment systems are comprised of seven integrated components:
    - **Camera, lens, and mount** — the basic function of the camera and lens system is to convert an optical image of the physical scene into an electrical (video) signal that is suitable for transmission to the alarm communication and display system's central repository.
    - **Lighting system** — the function of the lighting system is to illuminate the assessment zone evenly with enough intensity to ensure adequate performance of the chosen camera system.
        - Light fixtures should be mounted well above camera height.
        - This prevents bright light sources from intruding on the camera's field of view.
    - **Video transmission system** — the overall function of a video transmission system is to connect the remote cameras to the local video monitors in such a way that there is no interference of the video signal.
        - Video transmission may be accomplished in several ways, to include coaxial cables, fiber optics, microwave links, and infrared systems.
        - It is important that the video transmission system used should have a bandwidth equal to or greater than the bandwidth of the cameras being used.
    - **Video switching equipment** — most alarm assessment systems use more cameras than display monitors.

    - For this reason, a video switcher is used to connect the multiple video signals coming from the cameras with one or more monitoring devices.
    - The simplest type of switcher connects one of a number of inputs to a single output, with one input connected at a time.
    - Multiple output switchers can switch one or more inputs to any combination of outputs.
  - **Video recorder** — the purpose of the video recording is to produce a record of an event. In addition to providing historical information for later review, it provides an aid to the real-time assessment by adding instant replay stop-action to the system.
  - **Video monitor** — provides a view of each assessment zone (both interior and exterior)
    - Each assessment zone should occupy 75 percent of the monitor area and should be centered on the screen.
    - This makes alarm assessment easier by presenting a consistent view to the operator.
  - **Video controller** — is the main interface between the alarm sensor system and the alarm assessment system; the controller automatically:
    - Regulates the inputs and outputs of the video switcher.
    - Keeps track of the recorder.
    - Displays scenes on the monitor.
- Explain that nontechnical solutions, such as visual checks from security force members, can aid and supplement video alarm assessment.

Slide 26 Alarm Assessment Components (2 of 3)

- *Video*

Graphic Description: Video of improper camera placement allowing intruder to avoid detection by using fence as a shield

- Click on the arrow below image to play the video.
- Explain that it illustrates improper camera placement.
- Point out how the intruder benefits from visual protection provided by the fence.

Slide 27 Alarm Assessment Components (3 of 3)

- *Video*

Graphic Description: Video of poor interior visibility due to poor interior lighting and sunlight reflections

- Click on the arrow below image to play the video.
- Explain that this illustrates the importance of proper interior lighting.
- Point out that poor lighting and reflections from sunlight can affect interior visibility.
- Ask participants whether they have any questions on alarm assessment or anything else covered this far.

Slide 28 Entry Control Systems (1 of 2)
▪ Permit entry and exit to only authorized personnel ▪ Detect and prevent entry or exit of contraband material ▪ Provide information to the security force ▪ Located at a facility's perimeter or interior
Graphic Description: Pin reader keypad to facilitate controlled access

- Explain the purposes of an effective entry control system:
  - Allow the movement of authorized personnel and material into and out of facilities.
  - Detect and possibly delay unauthorized personnel and contraband (for example, weapons, explosives, unauthorized tools, or critical assets).
  - Provide information, usually electronically, to the security force to facilitate assessment and response decisions.
- Explain that entry control elements are located at:
  - A facility's perimeter, for example, vehicle gates, and building entry points.
  - A facility's interior, for example, doors into restricted rooms or other special areas within a building.

Slide 29 Entry Control Systems (2 of 2)
▪ Performance is measured according to: • Flow rate — the measure of the time it takes for an authorized person or material to successfully pass an entry or exit point • Error rate — the percentage that a specific entry control technique or process **falsely rejects** an authorized person or **falsely accepts** an unauthorized person
Graphic Description: No Graphic

- Remind participants that *Module 12: Security Force Operations* covered the topic of entry control but not entry control systems.
- Define the following terms:
  - **Flow rate:** the measure of the time it takes for an authorized person or material to successfully pass an entry or exit point.
  - **Error rate:** the percentage that a specific entry control technique or process **falsely rejects** an authorized person or **falsely accepts** an unauthorized person
  - **Type I error:** the false rejection of an authorized person.
  - **Type II error:** the false acceptance of an unauthorized person.
- Explain that the performance of the entry control system is measured by flow rate and error rate.

Slide 30 Entry Control Systems Features (1 of 2)
▪ Prevents bypass ▪ Allows observation by security force members ▪ Protects the security force member ▪ Performs access and material control ▪ Blocks passage until access and material control are complete
Graphic Description: Safety gate with barrier fence, intercom, and card scanner

Slide 31 Entry Control Systems Features (2 of 2)
▪ Provides secondary inspection for those who cannot pass automated inspection ▪ Accommodates maximum flow of vehicles and people ▪ Provides central alarm station surveillance ▪ Allows facility entry and exit
Graphic Description: Long lines at airport security entry control stations

- Tell participants the features of an effective entry control system as shown on the slides.

Slide 32 Entry Control Systems Categories
▪ This section will cover: • Personnel entry control systems • Contraband detection systems • Locks
Graphic Description: No Graphic

- Tell participants the categories of entry control systems that will be discussed in the next slides.

Slide 33 Personnel Entry Control Systems (1 of 2)
▪ Verify the authorization of individuals seeking entry to a controlled area based upon whether the person seeking entry: • Knows a valid personal identification number • Carries valid credentials • Possesses physical characteristics that match database information ▪ Combinations of systems fortify protection
Graphic Description: No Graphic

Slide 34 Personnel Entry Control Systems (2 of 2)
▪ *No Text*
Graphic Description: Various types of biometrics

- Explain that personnel entry control systems verify the authorization of individuals seeking entry to a controlled area.
- Explain that the verification decision is usually based on whether the person seeking entry:
  - Knows a valid personal identification number (PIN).
  - Carries a valid credential (photo identification badges, exchange badges, stored-image badges, and coded credentials).
  - Possesses the proper unique physical characteristics that match information in a database (biometrics).
- Explain that, while combinations of these entry control systems can reduce flow rate, when used in combination they make the physical protection system more difficult to defeat.

Slide 35 Contraband Detection

- Examining personnel, materials, and vehicles to detect unauthorized items
  - Metal detectors
  - Package searches
  - Explosive detectors

Graphic Description: Officer and canine explosive detection team

- Define **contraband detection:** examining personnel, materials, and vehicles to detect unauthorized items using metal detectors, package searches, and explosive detectors.
- Tell participants that methods of contraband detection include:
  - Metal detectors
  - Package searches
  - Explosive detectors

Slide 36 Locks

- Used with other protection measures, such as security force checks and sensors
- Two major components:
  - Fastening device — secures the door in the closed or locked position
  - Coded mechanism — allows the movement of the bolt or latch to the unlocked position

Graphic Description: No Graphic

- Explain that locks provide an element of security, however, an individual with enough time and skill can defeat them.
  - Use locks in conjunction with other protection measures, such as security force checks and sensors.
  - Locks that are farther away from the face of the door are more protected.
    - To enhance lock protection, a guard plate can be used to cover as much of the lock cylinder as possible while still permitting the key to be turned.

    - Special security screws can be used to mount the hardware; screws that cannot be removed once installed provide the best protection, since an intruder is likely to have special tools for removable screws.
- Explain that the two major components in most locks include the following:
  - **Fastening device:** composed of a latch (or bolt) and the strike, which is the recessed area located in the doorjamb where the bolt or latch projects when the door is closed.
    - A latch is beveled and spring loaded so that it automatically retracts when the door is closed; the bolt is a uniformly thick device that stays in the same position unless it is intentionally moved.
    - Latches are more convenient and more vulnerable than bolts.
  - **Coded mechanism:** located in the lock body and, when decoded, permits movement of the latch or bolt, allowing it to retract into an unlocked position; the two types of coded mechanisms are:
    - **Keyless code:** operated by a code to gain access; codes include the following: mechanical combinations (number or letter dial rotated to certain positions in a particular order to gain access), electromechanical combinations (rely on electronics rather than mechanical parts), mechanical entry (allows entry based on pushing numbered buttons in a specific sequence), and electromagnetic (rely on strength of powerful electromagnets to secure a door)
    - **Key code:** operated by a mechanical key: when the correct key is used, the key and key mechanism both retract the bolt or latch, allowing access.
- Ask participants whether they have questions on entry control systems or anything else covered thus far.
- Explain that participants have just learned about the four required elements of the detection and assessment function:
  - Intrusion sensing
  - Alarm communication and display
  - Alarm assessment
  - Entry control
- Tell participants the next section covers how the second physical protection system function — delay — can use nontechnical solutions to delay unwanted intrusion.

Slide 37 TeachBack Moment

- What are the three characteristics of an effective physical protection system as they apply to technology?
- What are the performance characteristics of intrusion sensor systems?

Graphic Description: No Graphic

- Conduct a TeachBack moment to assess how well participants understand the content presented in this section of the module.
- Ask participants:
  - **What are the three characteristics of an effective physical protection system as they apply to technology?**
  - Acknowledge responses. *If not provided by participants, add the following:*

  - *Protection in depth*
  - *Minimum consequences of component failure*
  - *Balanced protection*
- **What are the performance characteristics of intrusion sensor systems?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Probability of detection*
  - *Vulnerabilities to defeat*

Topic: Primary Physical Protection System Functions — Delay	**30 Minutes**

Enabling Learning Objective:
- Explain how nontechnical solutions can be used to delay unwanted intrusion.

Slide 38 Primary Physical Protection System Functions — Delay (1 of 3)
▪ *No Text*
Graphic Description: Primary physical protection system functions diagram with Delay box highlighted in yellow

- Point out to participants where the Delay function falls on the diagram (block is highlighted in yellow).

Slide 39 Primary Physical Protection System Functions — Delay (2 of 3)
▪ Purpose: increase the time it takes for a terrorist to carry out an attack by placing obstacles along the intended path to the target ▪ Performance measure: time • Critical element of system effectiveness • Depends on barrier and penetration time • Detection systems and barriers should be adjacent
Graphic Description: No Graphic

- Explain that the purpose of delay barriers is to increase the time it takes for a terrorist to carry out an attack by placing obstacles along the intended path to the target — once an intruder has been detected, effective delay elements will prevent completion of plans for attack or provide sufficient delay for the response force to arrive.
- Explain that the performance measure for delay elements is **time**.
  - Delay after detection is an extremely critical element of system effectiveness.
    - Each additional minute the intruder is delayed provides additional time for assessment and for the response force to interrupt the action.
    - Early detection at a facility's perimeter (as opposed to detection inside the facility itself), combined with minimal time required to make an alarm assessment decision, increases the available response force time.
  - Delay time for the intruder will depend on the specific barrier to be breached and the tools the intruder uses to attempt defeat of the delay barrier.

  - Intruders penetrate barriers when they can pass through, over, under, or around the protective structure.
  - The penetration effort is assumed to start at a distance one meter in front of the barrier and ends at a point one meter beyond the barrier.
  - Penetration time is the amount of time it takes the intruder to overcome the barrier.
  - Barriers must be considered in relation to the intruder's objective.
  - If the objective is theft of critical assets, barriers that are penetrated or destroyed on the way into the facility may not provide delay for departure from the facility.
  - For example, some emergency exits provide delay from the outside, but due to safety requirements, allow rapid exit from the inside.
- To aid alarm assessment and interception of the intruder at predictable locations, install detection systems and barriers adjacent to each other so that the barrier is encountered immediately after a sensor is breached.

Slide 40 Primary Physical Protection System Functions — Delay (3 of 3)

- Passive barriers (fixed)
- Deployable barriers (operable)
- Personnel or security force

Graphic Description: No Graphic

- Tell participants the three types of barriers, as shown on the slide.
- Explain that a well-designed physical protection system will combine each of these barrier types to achieve maximum effectiveness.
- Emphasize that unlike the technical solutions presented earlier in this module for the detection element of a physical protection system; most of the barrier delay solutions are nontechnical in nature.

Slide 41 Passive Barriers

- Remain in place at all times
- Delay an attacker from completing the attack objective
- Are divided into two categories:
  - Perimeter
  - Structural

Graphic Description: No Graphic

- Explain that passive barriers:
  - Remain in place at all times (fixed or permanently installed)
  - Delay an attacker from completing the attack objective because of the time it takes the intruder to overcome the barrier
- Explain that passive barriers are divided into two categories:
  - Perimeter
  - Structural

Slide 42 Passive Barriers — Perimeter
▪ Purpose: prevent unauthorized entry ▪ Function: form the outermost protective layer of the physical protection system ▪ Types: fences, gates, vehicle barriers, and natural barriers
Graphic Description: No Graphic

- Tell participants the purpose of perimeter barriers is to keep unauthorized personnel from entering the critical infrastructure.
- Explain that perimeter barriers form the outermost protective layer of the physical protection system.
- Provide examples of perimeter barriers: fences, gates, vehicle barriers, and natural barriers — remind participants of any of these types of barriers they encountered on the way into the facility holding this course.

Slide 43 Fences (1 of 2)
▪ Common perimeter barriers ▪ Not always a strong deterrent but provide a visible legal boundary and warning ▪ Can increase delay time and allow response force time to interrupt and neutralize the intruder closer to the point of alarm
Graphic Description: Barbed wire fence

- Tell participants that passive perimeter barriers form the outermost protective layer of the physical protection system.
- Explain that fences are not considered a strong deterrent to intrusions.
  - Standard chain-link fences are common as perimeter barriers around a critical infrastructure facility.
  - They cannot be considered a serious deterrent because an intruder can easily defeat a fence by:
    - Ramming it with a vehicle
    - Climbing or bridging over it
    - Crawling under it
    - Cutting through it in a few seconds
  - Fence barriers do provide a visible legal boundary and can display signs warning an intruder of the consequences of trespassing.
- Explain that when properly reinforced, fences can be effective in increasing the delay time, which will allow the response force (security force) time to possibly interrupt and neutralize the intruder closer to the point of alarm, for example:
  - If a fence is reinforced with a vehicle barrier, such as aircraft cable, this forces an intruder initially attempting entry by vehicle to travel on foot and hand-carry any necessary tools and equipment.
  - Reinforcements like this increases delay time and allow the response force to possibly intercept the intruder closer to the point of the alarm.
  - Security fences topped with rows of barbed wire do not prevent intrusion but will increase intruder delay.

- Barbed wire can be placed horizontally on the inside of a fence to prevent accidental injury to the casual passerby.
- Where there is more than one fence providing protection (inner, middle, and outer fences), barbed-tape rolls can be placed horizontally on the ground or stacked vertically against the inner or middle fence fabric.
- While an intruder can still use a ladder to bridge over the barbed-tape rolls, this additional barrier will increase delay time.
- Prevent excessive plant growth and collection of debris in the barbed-tape rolls to ensure a clear closed-circuit television view is maintained continuously.

Slide 44 Discussion Question

- How could you strengthen perimeter fence use and increase delay time?

Graphic Description: No Graphic

- Ask participants: **How could you strengthen perimeter fence use and increase delay time?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Use a fence in conjunction with a vehicle barrier (which forces an intruder driving a vehicle to travel on foot and hand-carry attack breaching tools and attack equipment)*
  - *Place barbed wire on top of a fence or on the inside of a fence, in barbed-tape rolls*

Slide 45 Fences (2 of 2)

- *Video*

Graphic Description: Video of barbed-tape rolls being breached by bridging with ladder

- Click on the arrow below image to play the video.
- Explain that the video illustrates how intruders can quickly penetrate barbed-tape rolls placed along a fence by bridging over with a ladder.

Slide 46 Gates (1 of 2)

- Function:
  - Establish specific points of entry and exit to an area defined by fences and walls
  - Limit the flow of pedestrian or vehicular traffic and establish a controlled traffic pattern

Graphic Description: Pedestrian entry control gate

Slide 47 Gates (2 of 2)

- Easy to defeat if they have:
  - Weak hinges, locks, and latches
  - Driveways positioned directly in front of the gate (make ramming by vehicle easier)

Graphic Description: Gate of Buckingham Palace with foot guards

- Describe gates and their functions.
- Explain the reasons why gates are easy to defeat.

Slide 48 Discussion Question
▪ How could you strengthen perimeter gate use and increase delay time?
Graphic Description: No Graphic

- Ask participants: **How could you strengthen perimeter gate use and increase delay time?**
  - Acknowledge responses. *If not provided by participants, add the following:*
    - *Use interlocking gates (requiring one gate to be closed and locked before the other can be released and opened).*
    - *Construct driveways with multiple turns to reduce vehicle approach and departure speeds.*
    - *Use speed bumps in the area of the driveway that is directly in front of the gate to reduce vehicle speed.*

Slide 49 Vehicle Barriers (1 of 3)
▪ Function: restrict and control entry ▪ Design considerations: • Define the threat that the barrier system is intended to stop • Define the asset and determine area to be protected • Examine site-specific conditions
Graphic Description: No Graphic

- Explain that the entry of private, business, and delivery motor vehicles should be restricted since they can carry tools and explosives; as mentioned earlier; these vehicles can also be used to penetrate perimeter barriers.
- Explain that the following design considerations should be examined and coordinated regarding vehicle barrier systems:
  - Define the threat that the barrier system is intended to stop (height and weight of the vehicle, impact velocity, and other physical characteristics)
  - Define the asset and determine the area that should be protected
  - Examine site-specific considerations, such as terrain, road layout in and around the secured area, building and parking lots layout, climate conditions, and traffic patterns in the area

Slide 50 Vehicle Barriers (2 of 3)
▪ Install vehicle barriers that are difficult to defeat in areas that cannot be monitored continuously
Graphic Description: Concrete barriers in front of street entrance to government building

- Explain that vehicle barriers that are difficult to defeat should be installed in areas that cannot be monitored continuously. For example:
  - Deeply buried concrete-filled pipes can be constructed so they are difficult to defeat, delaying an intruder long enough to be detected.
  - Cable barriers, on the other hand, can be defeated with hand-carried cutting tools; these types of vehicle barriers should be located only within areas that are well patrolled or sensored, and under closed-circuit television assessment.
- Remind participants that *Module 12: Security Force Operations* explained the use of jersey barriers (concrete slabs approximately .8 m high with slanted sides used to block, reroute, or divide traffic); placing these vehicle barriers along the sides of a roadway leading to a facility will slow or prevent an intruder in a vehicle from leaving the road.

Slide 51 Vehicle Barriers (3 of 3)

- *Video*

Graphic Description: Video of trucks attempting to penetrate chain-link fence, chain-link fence reinforced with aircraft cable, concrete-filled posts, concrete highway barrier, and heavy equipment tire stacks

- Click on the arrow below image to play the video.
- Ask participants the following discussion question: **What examples can you provide of vehicle barriers that are difficult to defeat?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Chain-link fences reinforced with aircraft cables*
  - *Concrete-filled posts*
  - *Concrete highway barrier*
  - *Heavy equipment tire stacks*
- Show video clip and explain that it illustrates how chain-link fence alone provides no penetration resistance compared to other vehicle barriers.
- Ask participants whether they have any questions about the use of vehicle barriers or anything else covered thus far.

Slide 52 Natural Barriers

- Water
- Vegetation
- Ditches or trenches
- Hard-to-access terrain

Graphic Description: Alcatraz Island, San Francisco, California, US

- Explain that natural barriers are those found in an exterior environment, for example:
  - Water, such as lakes, ponds, and moats
  - Vegetation, such as dense bushes, rows of trees, thorn or briar patches
  - Ditches or trenches
  - Hard-to-access terrain, for example rugged coastlines, high cliffs, and mountaintops

- Provide two examples of natural water barrier use:
  - Alcatraz, the small island located in the United States in the middle of the San Francisco Bay, California, US
    - Alcatraz initially served as a lighthouse.
    - Due to the natural water barrier, it was an excellent selection for a military post as well as a federal prison because any incoming adversary could be observed well in advance of landing on the island.
  - Nuclear power plants require water to be in close proximity.
    - The water of the ponds, lakes, or rivers serves the purpose of cooling the towers through recirculated water.
    - The water also makes it difficult for an adversary to approach the power plant by way of the waterway without being observed by security force members.
- Ensure that vegetative growth does not obstruct closed-circuit television camera view or reduce security force's ability to see those who are approaching; clear away any excess vegetation.

Slide 53 Discussion Question
▪ What examples can you provide of natural barriers for critical infrastructure facilities in your country?
Graphic Description: No Graphic

- Ask participants: **What examples can you provide of natural barriers for critical infrastructure facilities in your country?**
- Acknowledge responses. *Responses will vary.*

Slide 54 Passive Barriers — Structural (Workbook 13.3) 
▪ Walls ▪ Doors ▪ Windows and utility ports ▪ Roofs and floors
Graphic Description: No Graphic

Slide 55 Discussion Questions
▪ How can using two or more concrete walls in a series increase delay time? ▪ How can you reinforce doors to increase penetration resistance? ▪ How can you increase window penetration resistance? ▪ Why do floors offer more penetration resistance than roofs?
Graphic Description: No Graphic

- Remind participants that they reviewed passive structural barriers and standards in *Module 11: Policies and Procedures*.
- Refer participants to **Workbook 13.3: Passive Structural Barrier Modifications.**

- **Note:** use the addendum to discuss each of the types of structural barriers and answer the discussion questions at the end of each section.
  - **Walls:**
  - Ask participants: **How can using two or more concrete walls in a series increase delay time?**
    - Acknowledge responses. *If not provided by participants, add the following:*
    - *The intruder would have to penetrate each wall separately and transport breaching tools through each wall.*
    - *If explosives are used, the explosive charge may cause roof and other structural collapse, creating a barrier of rubble.*
  - **Doors:**
  - Ask participants: **How can you reinforce doors to increase penetration resistance?**
    - Acknowledge responses. *If not provided by participants, add the following:*
    - *Use steel plates and reinforced hinges, frames, and hardware.*
  - **Windows and utility ports:**
  - Ask participants: **How can you increase window penetration resistance?**
    - Acknowledge responses. *If not provided by participants, add the following:*
    - *Install steel grates over the windows.*
    - *Use reinforced frames that resist cutting tools.*
    - *Reposition the window's locking mechanism so that it is not readily accessible from the outside.*
    - *Use reinforced locking mechanisms.*
    - *Install windows that do not open.*
    - *Add thickness to the window or use wire mesh or polycarbonate glazing.*
  - **Roofs and floors:**
  - Ask participants: **Why do floors offer more penetration resistance than roofs?**
    - Acknowledge responses. *If not provided by participants, add the following: because floors are protected by the main structure and are designed to withstand heavier loads than roofs.*
- Ask participants whether they have questions about passive barriers (perimeter or structural) or anything else covered thus far.

Slide 56 Deployable Barriers
▪ Deployed: • When threat level is high • Very close to the protected asset ▪ Operate using two types: • Active — activated on command • Passive — activated automatically ▪ Allow security force time to respond to threat
Graphic Description: Two examples of deployable concrete highway barriers known as Jersey barriers

- Define **deployable barriers**: an obstacle that is only activated:

  - When threat level is high or when there is an actual attack
  - Very close to the protected asset since this is the most effective location for delay and deployment close to the target reduces cleanup efforts and collateral damage
- State the two operable types of deployable barriers.
  - **Active —** activated on command to stop or delay an intruder from completing the attack objective, such as an automated bollard.
  - **Passive —** activated automatically by penetration attempts
    - Provide an example of a passive deployable barrier from your own experience or provide the following example:
      - An intruder enters a room attempting to gain access to a safe containing classified information.
      - As the intruder crosses a sensored threshold and heads towards the safe, the sensor triggers razor wire to fall from the ceiling, encasing the safe.
- Explain that deployable barriers allow a security force time to respond to a threat or attack.
  - Deployable barriers only delay an intruder for a limited time — given sufficient time and the right tools, an intruder can defeat any delay mechanism.
  - The security force team must respond and achieve control in a shorter time than the deployable barrier time.

Slide 57 Discussion Questions
▪ Why are deployable barriers typically deployed very close to the protected asset? ▪ What advantage does a passive deployable barrier system have compared to an active deployable barrier system?
Graphic Description: No Graphic

- Ask participants:
  - **Why are deployable barriers typically deployed very close to the protected asset?**
  - Acknowledge responses. *If not provided by participants, add the following:*
    - *This is the most effective location for delay.*
    - *Close deployment reduces cleanup efforts and collateral damage.*
  - **What advantage does a passive deployable barrier system have compared to an active deployable barrier system?**
  - Acknowledge responses. *If not provided by participants, add the following:*
    - *Elimination of the command and control hardware significantly reduces the system's overall cost.*
    - *Since passive deployable barriers immediately deploy, this reduces alarm assessment time and increases time required for response.*

Slide 58 Bollards and Rising Wedge Barriers
▪ Bollards — fixed or retractable; often used in high-traffic entry and exit lanes ▪ Rising wedges — retractable and can be raised or lowered
Graphic Description: Two examples of bollards and wedge barriers

- Explain that bollards can be fixed, retractable, or removable and are commonly used in high-traffic entry and exit lanes.
  - Can be raised to allow only pedestrian traffic or lowered to allow vehicle traffic
  - Decorative on sidewalks for pedestrian traffic
  - May have a high crash rating for vehicular traffic
- Tell participants that rising wedge barriers are also retractable and can be raised or lowered.

Slide 59 Personnel or Security Force as Barriers
▪ Can serve as delay barriers if security force members: • Hold fixed positions • Are well-protected and well-trained • Are properly equipped • Have clear communication protocols
Graphic Description: No Graphic

- Explain that in addition to (or in the absence of) the passive and dispensable barriers, personnel can be deployed to create intruder delay — assigned members of the security force team can be considered an element of delay if personnel are in fixed and well-protected positions.
- Explain that for personnel to be effective delay barriers, they must be well-trained and properly equipped.
- Explain that the security force communication equipment must be fully functioning and communication procedures must be in place in order for the pre-positioned security force members to have as much advance warning as possible about the intruder's projected path.
  - Procedures and protocols include the need to provide status reports regarding progress of intruder attempt interruption.
  - This is particularly important in instances where additional back up is needed or emergency medical attention is required.
  - As is the case with initial notification of detection, deployed security force members usually use two-way radios to communicate status or additional needs.
- Remind participants that other elements that contribute to security force effectiveness were presented in *Module 12: Security Force Operations*.

Slide 60 Discussion Question
▪ What other factors affect the security force's ability to serve as an effective delay barrier?
Graphic Description: No Graphic

- Ask participants the following discussion question:
  - **What other factors affect the security force's ability to serve as an effective delay barrier?**

  - Acknowledge responses. *If not provided by participants, add the following:*
    - *Proper security equipment*
    - *Current training*
    - *Fully functioning communication equipment*
    - *Clear communication procedures*
- Ask participants whether they have questions on barrier delay systems or anything else covered thus far.
- Summarize this entire section on the delay function of the physical protection system by reminding participants that they have learned about the three types of delay barriers which include passive barriers (perimeter and structural), deployable barriers (active and passive), and personnel (security force).
- Tell participants the next section covers the third physical protection system function, response, as it relates to technology.

Topic: Primary Physical Protection System Functions — Response	**20 Minutes**

Enabling Learning Objective:
- Explain the elements of a security technology plan for an unwanted intrusion to protect critical infrastructure.

Slide 61 Primary Physical Protection System Functions — Response (1 of 2)
▪ *No Text*
Graphic Description: Physical protection system functions diagram with Response box highlighted in yellow

- Show participants where the response function falls on the diagram (block is highlighted in yellow).
- Remind participants that detailed information about security force effectiveness was already presented in *Module 12: Security Force Operations*; therefore, the response function of the physical protection system will only be covered briefly in the upcoming section.
- Review the interrelationship between the three elements of response, as shown on the diagram, by asking participants the following discussion question:
  - **How is the security force's overall effectiveness measured in relation to the three elements of the response function?**
  - Acknowledge responses. *If not provided by participants, add the following: the time between receipt of communication of intruder action and the interruption of the terrorist action.*

Slide 62 Primary Physical Protection System Functions — Response (2 of 2)
▪ *No Text*
Graphic Description: Response function of the physical protection system flow chart

- Refer to the figure on the slide and explain the three elements required to prevent terrorist success.
  - Communicate information to security force — response force time includes the time it takes for the security force to receive communication about a terrorist threat
  - Deploy security force — response force time includes the time it takes for the security force to deploy and establish its position to interrupt terrorist activity
  - Interrupt terrorist activity
- Remind participants that they learned about neutralization in *Module 12: Security Force Operations*.
  - Neutralization is the point at which terrorists' actions are stopped and terrorists are no longer able to fight against the security force.
  - In some high-security applications, neutralization may also be a measure of security force success.

Slide 63 Communicate Information to Security Force (1 of 2)
▪ Frequency modulation or two-way radio is the most common method to communicate with the security force ▪ Advantages include: • Allow rapid reporting and deployment • Easy to operate • Efficient • Inexpensive
Graphic Description: No Graphic

Slide 64 Communicate Information to Security Force (2 of 2)
▪ Disadvantages include: • Range limitation (overcome by the use of repeaters and multiple-receive systems) • Vulnerability to eavesdropping, deceptive messages, and jamming (overcome by a spread-system or frequency-hopping communication system)
Graphic Description: Antenna on high ground

- Remind participants that they discussed in *Module 12: Security Force Operations* that the most common means of communicating with the security force is through clear-voice two-way radios, normally of the frequency modulation type.
- Explain the advantages of two-way radios — when proper transmission procedures are followed, routine communications using this system can be conducted successfully.
  - Allow rapid reporting:
    - Low-power, battery-operated, handheld radios that allow rapid reporting of conditions found during routine patrols.
    - Enable rapid deployment of the security force during security events.
  - Easy to operate
  - Efficient
  - Inexpensive

- Tell participants the disadvantages of two-way radios.
  - **Range limitation:**
    - Inadequate range is the biggest deficiency of this system.
    - To minimize this deficiency, repeaters or a multiple-receiver system can be used.
    - A repeater receives voice transmissions from the handheld units and transmits them again on a separate frequency to all other units within the system.
    - By placing the repeater at a higher location, the range of the radios increases.
    - A multiple receiver system consists of several remotely located receivers connected to the central monitoring station by a landline.
    - A microcomputer monitors the signals received by all multiple receivers and transfers the information to the central station from the remote receiver receiving the strongest signal.
  - **Vulnerability to eavesdropping, deceptive messages, and jamming:**
    - Jamming occurs when an intruder knows the frequency on which the security force is operating.
    - The right frequency is not difficult to determine, as terrorists can use simple equipment (scanners) to test every frequency until they find the right one.
    - The terrorist then sends out sound waves at a similar frequency, which interferes with the security force's signal.
    - Jamming prevents the ability to send or receive communication or distort messages so they cannot be understood.
    - One method to counteract terrorist eavesdropping, deception, and jamming is the spread-spectrum or frequency-hopping communication system.
    - In this system, the master transmitter makes the other receivers follow it automatically from channel to channel as the message is transmitted.
    - For any particular receiver in the system, the message is received like any other continuous message.
    - For an intruder, however, the transmission is going to sound like bits and pieces making the message impossible to understand.
    - Alternate means of communication, such as intercoms, public address systems and cell phones should be available at all times.

Slide 65 Deploy Security Force
▪ Responding personnel ▪ Contingency planning ▪ Communications ▪ Interruption and neutralization
Graphic Description: No Graphic

- Remind participants of the components of the response function from *Module 12: Security Force Operations*:
  - Responding personnel
  - Contingency planning
  - Communications
  - Interruption and neutralization

Topic: Threaded Exercise Part 6 — National Ministries Building **60 Minutes**

Slide 66 Threaded Exercise Part 6 — National Ministries Building (Workbook Part 6)

- Purpose: to develop a security technology plan for the protection of the National Ministries Building
  - Duration: 60 minutes (40-exercise; 20-debrief)
  - Group composition: table groups
  - Debrief: discussion

Graphic Description: No Graphic

Slide 67 National Ministries Building Complex Map (Workbook Part 6)

- *No Text*

Graphic Description: National Freedom Building map and buildings

- Refer participants to **Threaded Exercise Part 6 — National Ministries Building** and allow a few minutes for the participants to read the instructions.
- Tell participants that instructions will refer them back to the sections from:
  - *Module 10: Analyzing the Threat*, **Part 3: Threat Analysis —** Adjacent Country Intelligence Report
  - *Module 6: Critical Infrastructure Assets*, **Part 2: Critical Infrastructure Assets** — Facility Director's Second Response Letter
- Read the finalized threat analysis statements for the Urban Front terrorist organization, the Union Workers for a Better Life activist group, and the Intelligence Bulletin.
- Conduct the exercise as follows:
  - Emphasize to the teams that their security technology plans should be based on information presented in *Module 10: Analyzing the Threat*, **National Ministries Building Data Collection in Part 3: Threat Analysis**:
    - The Adjacent Country Intelligence Report and the finalized threat analysis statements
    - Letter from National Ministries Building Facility Director in Response to Data Call
    - The additional Intelligence Bulletin added in this module
  - Assign an interpreter to each team as needed.
  - Explain that cost is not a factor at this point; participants can recommend any solutions that appear to effectively prevent or mitigate the threat. Note: While participants have an unlimited budget now, they will scale back their recommendations during *Module 15: Operational Resilience*.
  - Emphasize that while the focus is on technical solutions, the teams can also recommend:
    - Nontechnical solutions
    - Related policies and procedures

- The teams should be prepared to discuss their security technology plan and explain the rationale used for resulting solutions during their presentation in Part 8.
- Refer to **Threaded Exercise Workbook Part 6 — National Ministries Building Answer Key** for use during the discussion.
- As groups work, facilitators should walk around the room and answer any questions participants may have.

Topic: Module Summary	**10 Minutes**

Slide 68 Module Summary
▪ Characteristics of a physical protection system ▪ Primary physical protection system functions — detection and assessment ▪ Primary physical protection system functions — delay ▪ Primary physical protection system functions — response
Graphic Description: No Graphic

- Summarize the module by reviewing the following points:
  - **Characteristics of a physical protection system**
    - Protection in depth
    - Minimum consequences of component failure
    - Balanced protection
  - **Primary physical protection system functions — detection and assessment**
    - Exterior and interior intrusion sensors
    - Video alarm assessment
    - Entry control and alarm communication
    - Supplement the existing security force
  - **Primary physical protection system functions — delay**
    - Passive barriers (fixed)
    - Deployable barriers (operable)
    - Personnel or security force
  - **Primary physical protection system functions — response**
    - Communicate information to security force
    - Deploy security force
    - Interrupt terrorist activity
- Ask whether there are any questions about the contents of this module.
- Explain that *Module 14: Security Inspection and Validation* will describe how to develop a security inspection and validation program.