MODULE 12: SECURITY FORCE OPERATIONS

Day: 6 **Time:** 3.5 Hours **Level of Understanding:** Application

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

Module Equipment/Facilities:
- Standard Classroom Setup
- Workbook 12.1: Physical Protection System Functional Relationships Answer Key
- Threaded Exercise Workbook Part 5 — National Ministries Building Answer Key
- National Ministries Building Complex Map

Participant Materials/Handouts:
- Workbook 12.1: Physical Protection System Functional Relationships
- Workbook 12.2: Desirable Qualities in Security Force Personnel
- Workbook 12.3: Sample Security Force Response Plan
- Threaded Exercise Workbook Part 5 — National Ministries Building

Terminal Learning Objective

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

Introduction

Once the threat analysis statement is completed, you should then conduct an evaluation of the security countermeasures. This evaluation ensures that you are providing the appropriate level of security to protect the critical infrastructure from the terrorist threats identified in the threat analysis. In this module, the next security countermeasure you will evaluate is the security force. The security force's effectiveness depends on the ability to operate within established policies and procedures *(Module 11: Policies and Procedures)* and on the ability of technology to detect and assess intrusions and provide adequate delay *(Module 13: Security Technology)*.

During this module, you will learn the operational purpose of the security force: providing a sufficient force to interrupt intruder actions and to neutralize intruders before they achieve their goal(s). The security force response is dependent on having prearranged tactical plans, effective communication operations (to include procedures and equipment), and realistic training. You will have the opportunity to develop a security force response

plan for a given critical infrastructure that considers these needs. The security force response plan will help you protect against terrorist attacks.

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
Relationships between Functions	▪ Explain the functional relationships between detection and assessment, delay, and response. ▪ Explain the terms interruption and neutralization as they apply to security force effect.	45 minutes
Primary Elements of Security Force Effectiveness	▪ Describe the primary elements that contribute to a security force's effectiveness.	45 minutes
Develop a Security Force Response Plan	▪ Describe the format of a security force response plan.	15 minutes
Threaded Exercise Part 5 — National Ministries Building	▪ Develop a security force response plan for a given facility.	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
Assessment	A necessary step in the detection process to ensure whatever caused the alarm can be identified
Contingency planning	A method to develop well-documented procedures for identifying potential targets, responding to potential threats, interacting with external agencies, and determining the level of use-of-force security can use in various situations
Delay	The process of slowing down intruders' progress by increasing the time it will take intruders to achieve their goal

Key Term	Description
Deployment	The actions of the security force from the time communication is received that an intruder is attacking until the security force is in position to interrupt the intruder's actions
Detection	A process in which an alarm sensor activates due to an intruder attack, a nuisance alarm, or false alarm
Deterrent	Delay prior to detection; no value added to physical protection system
Entry control	A way to allow only authorized personnel and materials to enter the facility; detects and prevents attempted entry of unauthorized personnel and material
False acceptance rate	A measure of effectiveness of entry control; the frequency at which false identities or credentials are allowed entry (3 out of every 1000 entries)
False alarm	Any alarm where the cause of activation cannot be determined
False rejection rate	A measure of effectiveness of entry control; the frequency at which access to authorized personnel is denied (1 out of every 1000 entries)
Interruption	The successful arrival of the security force at an appropriate location and in sufficient numbers to confront the intruder(s)
Neutralization	The point at which intruders' actions are stopped and intruders are no longer able to fight against the security force
Nuisance alarm	Any alarm not caused by an intrusion
Protected paths	Routes and areas that have been secured for security force response
Response	The actions taken by the security force to prevent intruder success
Throughput	A measure of effectiveness of entry control; the number of authorized personnel allowed access per unit of time

Topic: Module Introduction — 5 Minutes

Slide 1 Security Force Operations

- 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: because the content of this module presents updated material from participants' current skill set, there are occasions to present the same information in more than one format or location. Take advantage of these opportunities for review to strengthen the participants' understanding of the new methods.

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 force response plan for the protection of critical infrastructure

Graphic Description: No Graphic

- Briefly discuss the terminal learning objective.
- Highlight the key topics to be presented:
  - Functional Relationships
  - Primary Elements of Security Force Effectiveness
  - Develop a Security Force Response Plan
- Ask participants whether they have any questions about anything covered thus far.

Slide 3 Physical Protection System

- *No Text*

Graphic Description: PPS diagram with Identify Security Countermeasures box highlighted in yellow

- Point out VAM Phase 3 on the slide, then down to where security force operations appears on the diagram beneath the Identify Security Countermeasures box.
- Remind participants that security countermeasures consist of policies and procedures, security force, technology, and security inspection and validation.
- Explain that this module discusses security force operations.

Topic: Relationships between Functions — 45 Minutes

Enabling Learning Objectives:
- Explain the functional relationships between detection and assessment, delay, and response.
- Explain the terms interruption and neutralization as they apply to security force effect.

Slide 4 Physical Protection System — Functional Relationships

- **Detection and assessment** — a successful detection of an intruder would result in sending in a response force
- **Delay —** once detected, the intruder must be delayed to allow time for the response force to arrive
- **Response —** the response force will neutralize the intruder

Graphic Description: No Graphic

- Remind participants that in *Module 2: Introduction to Critical Infrastructure Security and Resilience*, introduced them to the relationship between detection and assessment, delay, and response, as listed on the slide.
- Define:
  - **Detection:** a process in which an alarm sensor activates due to an intrusion, a nuisance alarm, or false alarm
  - **Assessment**: a necessary step in the detection process to ensure whatever caused the alarm can be identified

Slide 5 Intruder Action Timeline Activity (Workbook 12.1)

- Purpose: to organize intruder actions in the correct order
  - Duration: 10 minutes (5-activity; 5-debrief)
  - Group composition: individuals
- Debrief: large-group discussion

Graphic Description: No Graphic

- Refer participants to **Workbook 12.1: Physical Protection System Functional Relationships**, **Part 1: Intruder Action Timeline Activity**.
- Explain that this brief scenario activity represents an intruder timeline for stealing valuable information from a critical infrastructure.

- Tell participants they are to work individually to reorganize the list of intruder actions into the correct order in which the actions occurred using the list provided.
- Allow five minutes for the activity.
- Ask one or two participants to share their list.
- Refer to these actions as the functions of detection and assessment, delay, and response are discussed in the next two diagrams.

Slide 6 Relationships between Functions (1 of 2) (Workbook 12.1)

- *No Text*

Graphic Description: Detection and assessment, delay, and response comparison diagram

- Refer participants to **Workbook 12.1: Physical Protection System Functional Relationships, Part 2: Physical Protection System Functional Relationships Diagram**.
- Explain the relationship between detection and assessment, delay, and response:
  - For the physical protection system to be effective, it is imperative that each element function as designed: there must be notification of an attack (detection and assessment) and then progress of the intruder must be slowed (delay) that will allow the security force time to interrupt, stop, or neutralize the intruder (response).
- Tell participants that the diagram on the slide illustrates how detection and response time factors into the intruder's time.
- Explain that when an attack occurs involving a team of intruders, the detection, delay, and response functions are affected; the security force leader will typically make adjustments, according to the number of attackers and the attack methods used.
- Explain that the total time required for the intruder to accomplish the entire planned goal (labeled Terrorist task time) depends on the delay advanced by the security force.

Slide 7 Relationships between Functions (2 of 2)

- *No Text*

Graphic Description: Detection and assessment, delay, and response no interruption diagram

- Tell participants that this diagram represents the intruder in the activity completed his or her task without interruption.

Slide 8 Detection and Assessment Function (1 of 2)

- Detection and assessment — the first function of the physical protection system
- Detection without assessment is **not** detection

Graphic Description: No Graphic

Slide 9 Detection and Assessment Function (2 of 2)
▪ This section will cover: • Detection with electronic sensors • Detection with entry control • Detection with security force personnel
Graphic Description: Security camera

- Explain that detection and assessment is the first function of the physical protection system.
- Remind participants that *Module 2: Introduction to Critical Infrastructure Security and Resilience*, explained that detection is the discovery of an intruder action that includes sensing of covert or overt actions.
- Tell participants that detection without assessment is **not** considered true detection.
- Explain that this section will focus on various ways to accomplish detection through electronic sensors, entry control, and security force operations.

Slide 10 Detection with Electronic Sensors (1 of 2)
▪ A sensor reacts to a stimulus and initiates an alarm ▪ Sensor information is reported and displayed ▪ A qualified person assesses information and judges the alarm to be either an attack, a **nuisance alarm,** or a **false alarm**
Graphic Description: Motion sensor

Slide 11 Detection with Electronic Sensors (2 of 2)
▪ *No Text*
Graphic Description: Flow chart indicating detection with sensors process

- Explain that detection is not an instantaneous event, but a process in which:
  - A sensor reacts to a stimulus and initiates an alarm
  - Sensor information is reported and displayed
  - A qualified person assesses information and judges the alarm to be either an attack, a **nuisance alarm,** or a **false alarm**
- Define:
  - **Nuisance alarm**: any alarm where the cause of activation cannot be determined
  - **False alarm**: any alarm not caused by an intrusion
- Explain that once the detection systems (sensors) activate, assessment is a necessary step in the process to ensure identification of whatever caused the alarm.

Slide 12 Detection with Electronic Sensors Example (1 of 2)
▪ An intruder scales a fence that has a sensor attached ▪ Sensor activation communicates electronically to the security control center
Graphic Description: No Graphic

Slide 13 Detection with Sensors Example (2 of 2)
▪ Closed-circuit television on the fence line transmits an image of the intruder to the security control center monitors ▪ The security control center operator assesses the situation ▪ The response is to send security force members to the area
Graphic Description: Man reviewing a bank of monitors

- Explain the use of sensors for detection and assessment using the detection example scenario to demonstrate:
  - An intruder scales a fence that has a sensor attached
  - The sensor activation communicates electronically to the security control center
  - Closed-circuit television on the fence line reports a visual of the intruder back to the security control center monitors
  - The security control center operator assesses the situation and responds according to established policies and procedures by sending security force members to the area
- Tell participants that the previous example depicts the best-case scenario.
- Explain that in many cases closed-circuit television may not be available for assessment and the security control center operator must dispatch a security force member to the area to assess what caused the sensor activation.
- Explain that assessment by a security force member creates two immediate problems:
  - First, the member will take additional time to respond to the affected area, which allows the intruder more time to reach the target (asset).
  - Second, the intruder may not leave any signs of being there, which means the security force member may not accurately assess what occurred, in this case, an intruder(s) scaling the fence.
- Explain that if in the same scenario, a large animal touches the fence and it is not assessed as a nuisance alarm, detection has not occurred.
- Remind participants that detection without assessment is not considered detection.

Slide 14 Detection with Entry Control (1 of 2)
▪ **Entry control**: • Allows only authorized personnel and materials to enter the facility • Detects and prevents attempted entry of unauthorized personnel and material • Often conducted through use of technology
Graphic Description: Security guard scanning woman with metal detector

Slide 15 Detection with Entry Control (2 of 2)
▪ Effectiveness measured by: • **Throughput**: number of authorized entries per time unit • **False acceptance rate**: frequency of unauthorized persons allowed entry • **False rejection rate**: frequency of authorized persons denied entry
Graphic Description: No Graphic

- Explain the terms for entry control and its measurement.
- Define **entry control:** a way to allow only authorized personnel and materials to enter the facility; detects and prevents attempted entry of unauthorized personnel and material.
- Tell participants that entry control is often conducted through technology; however, it is imperative that security force personnel be available for immediate response to potentially intercept or interrupt and neutralize the intruder.
- Tell participants that the measures of effectiveness of entry control are throughput, false acceptance rate, and false rejection rate.
- Define:
  - **Throughput**: a measure of effectiveness of entry control; the number of authorized personnel allowed access per unit of time (for example 10 people per hour, assuming that all personnel who attempt entry are authorized for entrance).
  - **False acceptance rate**: a measure of effectiveness of entry control; the frequency at which false identities or credentials are allowed entry (3 out of every 1000 entries).
  - **False rejection rate**: a measure of effectiveness of entry control; the frequency at which access to authorized personnel is denied (1 out of every 1000 entries).

Slide 16 Detection with Security Force
▪ Personnel at fixed posts or on patrol may sense an intrusion ▪ Using an effective assessment system, security personnel provide: • Information about whether the alarm is valid • Details about the cause of the alarm
Graphic Description: No Graphic

- Explain how security force personnel can be a means of detection and assessment.
  - Guards at fixed posts or on patrol may serve a critical role in sensing an intrusion.
  - Then using an effective assessment system, the security force provides two types of information associated with detection:
    - Information about whether the alarm is a valid alarm or a nuisance alarm.
    - Details about the cause of the alarm — what, who, where, and how many.
- Tell participants that even when assisted by a video assessment system, however, humans do not make good detectors. Studies have shown that human observers using video monitors miss 48% of brief instances of movement.

Slide 17 Detection Function Effectiveness (1 of 2)

- Three elements:
  - Probability of sensing an alarm activation
  - Time required for reporting and assessing an alarm
  - Nuisance or false alarm rate
- The shorter the time between sensor activation and alarm assessment the more the probability of detection increases

Graphic Description: No Graphic

- Explain the measure of effectiveness for the detection and assessment function is based on the following elements:
  - Probability of sensing intruder action
  - Time required for reporting and assessing the alarm
  - The nuisance or false alarm rate
- Explain that the probability of detection:
  - Decreases as the time before assessment lengthens.
  - Increases when the delay between sensor activation and security personnel assessment is shorter.
  - Decreases when there is a long delay time between detection and assessment lowers the probability of detection.
- Explain that the more time is required to make an accurate assessment, the less likely it will be that the cause of the alarm is still present.
  - For example, if sensor alarms are assessed by sending a guard to the sensor location, by the time the guard arrives, the source of the alarm may be gone.
  - If this happens, the delay between sensor initiation and assessment was so lengthy that no assessment could be made.
- Tell participants that a longer delay between detection and assessment favors the intruder because it allows the intruder to move closer to the target before the security force is notified of an attack.
- Explain that the nuisance alarm rate is another performance measure of sensors.
  - In an ideal sensor system, the nuisance alarm rate would be zero.
  - However, in the real world, all sensors interact with their environment, which includes natural, industrial, and false alarms generated by the equipment itself.
- Tell participants that sensors cannot discriminate between intrusions and other events in their detection zone. This is why alarm assessment is essential.

Slide 18 Detection Function Effectiveness (2 of 2)

- *No Text*

Graphic Description: Video of Russian train station bombing

- Tell participants that this video is of a train station in Volgograd, Russia, December 29, 2013.
  - There were 18 killed and 44 wounded as a result of the attack.
  - The bomber used approximately 10 kilograms of TNT in a backpack bomb.

- **Click the image on the slide to play the video.**
- Tell participants to note that the security force officer noticed unusual behavior by the bomber.
  - The officer reached his arm out to stop the bomber before the bomber passed through the security checkpoint and entered the crowded facility.
  - The bomber then detonated at the checkpoint instead.

Slide 19 Discussion Questions
▪ What are some natural sources of nuisance alarms? ▪ What are some industrial sources of nuisance alarms? ▪ What are some sources for false alarms?
Graphic Description: No Graphic

- Ask participants: **What are some natural sources of nuisance alarms?**
- Acknowledge responses: *If not provided by participants, add the following:*
  - *Overgrown vegetation*
  - *Wildlife walking into the alarm path*
  - *Strong winds causing a nearby tree branch to be blown down onto an alarmed fence*
- Ask participants: **What are some industrial sources of nuisance alarms?**
- Acknowledge responses: *If not provided by participants, add the following:*
  - *Ground vibration*
  - *Electromagnetic interference*
- Ask participants: **What are some sources for false alarms?**
- Acknowledge responses: *If not provided by participants, add the following:*
  - *Poor design*
  - *Inadequate maintenance*
  - *Component failure*
  - *Dead batteries causing equipment malfunction*

Slide 20 Delay Function
▪ Definition: the process of slowing down intruders' progress by increasing the time it will take intruders to achieve their goal ▪ Purpose: increase the time it takes intruders to achieve their goal
Graphic Description: No Graphic

- Remind participants that second function of the physical protection system is delay.
- Define **delay function**: the process of slowing down intruders' progress by increasing the time it will take intruders to achieve their goal.
- Explain that the primary purpose of delay is to increase the time it will take intruders to achieve their goal. Thus, delay helps meet the physical protection system objective: ensure that an adequate security force arrives in time to prevent intruders from accomplishing their goal.

Slide 21 Delay Function Elements (1 of 2)
▪ Barriers — walls, doors, and other solid structures between intruder and target ▪ Locks — delay mechanisms within a barrier
Graphic Description: Man at locked door

Slide 22 Delay Function Elements (2 of 2)
▪ Activated delays — introduction of chemical elements as a delay (pepper spray, gas, or smoke) ▪ Personnel — security force members in fixed and well-protected positions
Graphic Description: No Graphic

- Explain that elements of the delay function include:
  - **Barriers** — this delay element typically includes walls, doors, and solid structures between the intruder and the asset (target).
  - **Locks** — in cases where the barrier delay is too strong, an intruder may attack a weaker point on the barrier such as the locks used. Locks and locking devices are normally easier to defeat than the whole barrier structure.
  - **Activated delays** — this element can include introduction of chemical weapons such as pepper spray, gas, or smoke.
  - **Personnel** — the security force can be considered an element of delay, if personnel are in fixed and well-protected positions. The goal of these personnel would be to delay the intruder's progress until the full security force response team arrives.

Slide 23 Delay Prior to Detection
▪ **Deterrent** — barriers placed before detection ▪ Forces intruders to consider another method ▪ No value to the effectiveness of the physical protection system
Graphic Description: Large fence around a building

- Explain that there are some situations where barriers are placed before detection to force intruders to change or abandon their tactic.
- Define **deterrent:** delay before detection.
- Tell participants that although the intruder is delayed, this delay is of no value to the effectiveness of the physical protection system. It does not provide additional time to respond to the intruder.
- Provide examples:
  - The use of low concrete or wooden ridges across driving pavement to limit the speed of a vehicle.
  - Placement of concrete slabs approximately .8 meters high with slanted sides used to block, reroute, or divide traffic along the sides of a road will slow or prevent an intruder in a vehicle from leaving the road.

Slide 24 Delay Function with Physical Protection System

- *No Text*

Graphic Description: Diagram of delay function of a physical protection system

- Explain how the diagram on the slide illustrates the function of delay just discussed in the physical protection system.
- Remind participants that the measure of delay effectiveness is the time required by the intruders after detection to bypass each delay to reach the asset and achieve their goal.
  - The delay function is most effective when the delay time for the intruders is more than the time required for the security force to respond and interrupt the intruders' actions.
  - However, if the delay time is not sufficient, the intruders have a distinct advantage over the security force.
  - Too little delay time allows the intruders more opportunity to reach the asset before the security force.
  - This, in turn, gives the intruders a greater chance of successfully accomplishing their goals.

Slide 25 Delay Function Example (1 of 2) (Workbook 12.1)

- An intruder scales a 2.5-meter fence and runs to the door of a critical infrastructure facility (2 minutes)
- Once at the door, the intruder breaks into the facility and runs down a hallway to an asset storage area (2 minutes)

Graphic Description: No Graphic

Slide 26 Delay Function Example (2 of 2) (Workbook 12.1)

- The intruder breaks into the asset storage area and steals critical information from the room (1.5 minutes)
- The intruder runs out of the facility using the same path used to enter (4 minutes)
- Total time for intruder to complete the task was 9.5 minutes

Graphic Description: No Graphic

- Refer participants to **Part 1: Intruder Action Timeline Activity** of **Workbook 12.1: Physical Protection System Functional Relationships.**
- Tell participants to enter the action times in the **Time** column as each action is discussed on the slides.
- Explain that it is critical to remember that the delay time clock does not begin until the intruder's actions are detected. If detection does not occur, the amount of delay built into the system will not make a difference.
- Tell participants that this example illustrates the concept of delay.
  - An intruder scales a 2.5-meter fence and runs to the door of a critical infrastructure facility. Total time is two minutes.

  - Once at the door, the intruder breaks into the facility and goes down a hallway to an asset storage area. Total time is two minutes.
  - The intruder breaks into the asset storage area and steals critical information from the room. Total time is one and a half minutes.
  - The intruder proceeds out of the facility using the same entrance path. Total exit time is four minutes.
  - Total time for intruder to complete task was 9.5 minutes.
- Tell participants that the intruder accomplishes the goal of stealing critical information in a total time of 9.5 minutes.
- Tell participants that any differences in detection or response times will affect the entire task timeline — for example, if the detection is upon opening the door instead of climbing the fence, how would that affect the timeline?
- Explain that the question then becomes, "Is there enough time for the security force to respond and interrupt the intruder before accomplishing the malevolent goal?" It depends on two factors:
  - When did detection start?
  - What is the security force's response time (worst-case location)?
- Tell participants that for the purpose of this example, the security force's worst-case location response time is 5 minutes. If effective detection occurred at the fence when the intruder was scaling it, the security force would interrupt the intruder's action inside of the asset storage area.

Slide 27 Discussion Questions
▪ What would happen if the intrusion sensor did not activate until the intruder reached the exterior door of the facility? ▪ As Chief of Security, what actions could you implement to lengthen the delay time to allow your security force more time to respond?
Graphic Description: No Graphic

- Ask participants: **What would happen if the intrusion sensors did not activate until the intruder reached the exterior door of the facility?**
- Acknowledge responses: *If not provided by participants, add the following:*
  - *The intruder would have additional time in the asset room, which could facilitate additional theft or facilitate an earlier exit.*
- Ask participants: **As Chief of Security, what actions could you implement to lengthen the delay time to allow your security force more time to respond?**
- Acknowledge responses: *If not provided by participants, add the following:*
  - *Harden the outside door of the facility to add delay time.*
  - *Harden the door into the asset storage room to add delay time.*
  - *Reduce the worst-case response time for the security force by adding a patrol.*

Slide 28 Response Function
▪ This section will cover: • Definition and success • Responding personnel • Contingency planning • Communication • Interruption • Neutralization
Graphic Description: No Graphic

- Explain that the third function of the physical protection system is the response — actions taken by the security force to prevent intruder success.
- Tell participants that this section will cover five components of the response function:
  - Responding personnel
  - Contingency planning
  - Communication
  - Interruption
  - Neutralization

Slide 29 Response Function Definition
▪ The actions taken by the security force to prevent intruder success
Graphic Description: No Graphic

- Define **response function**: the actions taken by the security force to prevent intruder success.

Slide 30 Response Function Success
▪ Established components: • Prearranged tactical plans • Communication devices • Realistic training ▪ Communication of accurate information and **deployment** of security force
Graphic Description: No Graphic

- Explain that security force success is dependent the following:
  - Having prearranged tactical plans
  - Communication devices
  - Realistic training
- Explain that response also includes communication to the security force of accurate information about intruder actions and the deployment of the security force.

- Define **deployment:** the actions of the security force from the time communication is received that an intruder is attacking until the security force is in position to interrupt the intruder's action.

Slide 31 Responding Personnel
▪ Depending on magnitude of attack, other responding personnel may include: • Contract security force members • Local and regional law enforcement, fire protection, and medical responders • Government agencies, in some cases
Graphic Description: No Graphic

- Explain that depending on the magnitude of the intruder attack, additional personnel may be required to assist the security force in their response. These may include the following:
  - Proprietary or contract guards
  - Local and regional law enforcement and fire protection
  - Government agencies, in some cases
- For example, an attack involving explosives that has injured employees at the target site will require not only a security force response but also that of fire and medical personnel.

Slide 32 Contigency Planning Definition
▪ A method to develop well-documented procedures for: • Identifying potential targets • Responding to potential threats • Interacting with external agencies • Determining level of use-of-force for various situations
Graphic Description: No Graphic

- Define **contingency planning**: a method to develop well-documented procedures for identifying potential targets, responding to potential threats, interacting with external agencies, and determining level of use-of-force for various situations.

Slide 33 Contigency Planning Purpose
▪ Provides procedures for responding personnel to evaluate the situation ▪ Allows: • Identification and evaluation of potential threats and intruder routes • Development of tactical plans for response • Planning for training exercises
Graphic Description: Aerial view of a building with surrounding area including roads and waterways

- Explain the purpose of contingency planning is to provide procedures for responding personnel to evaluate the situation. Because a response plan cannot address every possible event in an attack contingency planning is essential.
- Explain that once a target has been identified, contingency planning allows security force personnel to:
  - Identify and evaluate potential threats and intruder routes.
  - Develop tactical plans to address various threats and responses including security force patrol routes and schedules.
  - Plan training exercises.
- Explain that policies and procedures should be well established and practiced through periodic training exercises. If outside agencies are likely to participate in the response, joint training exercises should be planned and executed.

Slide 34 Communication (1 of 3)

- Critical component of response function
- Information must be transferred with speed and accuracy
- Messages to security force must include:
  - Information on intruder actions
  - Instructions for deployment

Graphic Description: Man looking at monitors and communicating on a radio

- Explain that communication is a critical component of the response function since every system function depends heavily on proper communication between all responding personnel.
- Tell participants that information must be transferred through the communications network with speed and accuracy.
- Explain that communication to the security force must contain:
  - Information on intruder actions.
  - Instructions for deployment.

Slide 35 Communication (2 of 3)

- Effectiveness is measured based on time and accuracy
- Time varies based on method of communication
- Probability of correct and current data being transmitted increases after the initial response

Graphic Description: No Graphic

- Tell participants that communication effectiveness is measured on the time required to relay messages and the accuracy of the information.
- Explain that the time after initial transmission of information may vary considerably depending on the method of communication. For example, radios are faster than telephones.
- Explain that after the initial response period, the probability of correct and current data communicated is increased.

- However, there can be some delay in establishing accurate communication due to human behavior.
- For example, on the first attempt to communicate, the security control center operator is alerted that there is a call but may not have heard all the relevant information. The security control center operator makes a request for a second transmission to repeat the information, and finally, the operator understands the call and asks for clarification.

Slide 36 Communication (3 of 3)
▪ Most commonly used method is a two-way or frequency modulation clear-voice radio ▪ Two-way radios can be heard or jammed by intruders ▪ To guard against intruder communication attacks, plan for the use of alternative communication methods or technologies
Graphic Description: Two-way radio

- Explain that the most common method of communication is a two-way or frequency modulation clear-voice radio. Clear voice means that the signal has not been encrypted or encoded.
- Explain that this radio is not secure so intruders can:
  - Use standard receivers and scanners to listen to transmissions and send deceptive messages
  - Insert an unwanted signal into the channel to mask the desired signal. This is known as jamming transmissions.
- Explain how the security force can guard against communication attacks:
  - Plan alternate communication methods
  - Use a frequency-hopping system to prevent intruders from hearing communications clearly
    - 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.

Slide 37 Interruption Response
▪ **Interruption**: the successful arrival of the security force at an appropriate location and in sufficient numbers to confront intruder(s) ▪ Using **protected paths** increases chances of successful interruption
Graphic Description: No Graphic

- Tell participants that the last segment of the response function is interruption.
- Define **interruption:** the successful arrival of the security force at an appropriate location and in sufficient numbers to confront the intruder(s).

- Explain that successful interruption can be enhanced by the use of deployment through known, protected paths.
- Define **protected paths:** routes and areas that have been secured for security force response.
- Explain that protected paths are used to ensure that the intruder does not take advantage of an unprotected path.
  - If a security force response path is not protected, the intruder could use tactics to reduce or stop the security force response.
  - For example, an intruder could easily set up an ambush on an unprotected path and wait for the arrival of the security force team; using protected paths increases chances of success to interrupt intruder actions.

Slide 38 Neutralization Response
▪ **Neutralization**: the point at which intruders' actions are stopped and intruders are no longer able to fight against the security force ▪ Force-on-force training beneficial but not typically necessary at industrial facilities
Graphic Description: Man on ground being handcuffed by a law enforcement officer

- Define **neutralization**: the point at which intruders' actions are stopped and intruders are no longer able to fight against the security force.
- Explain that while training for force-on-force may be beneficial, neutralization will not typically be necessary at industrial facilities.
  - In the case of sites where an armed encounter between the security force and the intruder is expected, the security force must be trained with force-on-force exercises.
  - Neutralization will not typically be necessary at industrial facilities because they are more heavily guarded with substantial firepower.
- Tell participants that just because an intruder is interrupted, does not mean they have been neutralized. For example, first responders on the scene may be able to interrupt or delay the intruder's actions, but may not be able to neutralize the intruder.

Slide 39 Response Function of the Physical Protection System
▪ Communicate information to security force ▪ Deploy security force ▪ Interrupt and neutralize intruder attempt
Graphic Description: Diagram of response function of the physical protection system

- Tell participants the diagram on the slide illustrates the response function of the physical protection system.
- Explain that for the security force to interrupt the actions of the intruder there must be a sufficient number of security force members at a specific location. The security force measures its response effectiveness by the probability of deployment to the intruder location and time required to deploy the security force.

Slide 40 Response Function Example (1 of 2)
▪ The security control center operator receives notice of an alarm activation and transmits the location over the radio to a responding security force member
Graphic Description: Officer at command control center

Slide 41 Response Function Example (2 of 2)
▪ The member responds to the designated area and stands by in a defensive posture to wait for the intruder ▪ The intruder arrives and is interrupted by the security force member
Graphic Description: Officer standing in front of site with law enforcement canine officer

- Explain that the following scenario provides an example of the response function:
  - The security control center operator receives notice of alarm activation and transmits the location over the radio to a responding security force member.
  - The member responds to the designated area and stands by in a defensive posture to wait for the intruder.
  - The intruder arrives and is interrupted and neutralized by the security force member.

Slide 42 Discussion Question
▪ Based on this response example, what type of events could have caused this scenario to be less than a desired outcome?
Graphic Description: No Graphic

- Ask participants: **Based on this response example, what type of events could have caused this scenario to be less than a desired outcome?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Poor communication between the responding security force member and the security control center operator.*
  - *The time it took the responder to reach the asset before the intruder.*
  - *If the alarm was activated on the entry route of the intruder and the intruder uses a different exit route, the responder may not encounter the intruder.*

Slide 43 TeachBack Moment 
▪ What are the functional relationships between detection and assessment, delay, and response? ▪ How do the terms interruption and neutralization apply to security force effect?
Graphic Description: No Graphic

- Conduct a TeachBack moment to assess how well the participants understand the content presented in this section of the module.

- Ask participants: **What are the functional relationships between detection and assessment, delay, and response?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Detection alerts to unauthorized entry.*
  - *Assessment is a necessary step in the detection process to ensure whatever caused the alarm can be identified.*
  - *Delay is the process of slowing down intruders' progress by increasing the time it will take intruders to achieve their goal.*
  - *Response is the actions taken by the security force to prevent intruder success.*
- Ask participants: **How do the terms interruption and neutralization apply to security force effect?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Interruption is the successful arrival of the security force at an appropriate location and in sufficient numbers to confront the intruder(s).*
  - *Neutralization is the point at which intruders' actions are stopped and intruders are no longer able to fight against the security force.*
- Ask participants whether they have any questions about elements of response or anything else covered thus far.
- Tell participants that the next section discusses elements of security force effectiveness.

Topic: Primary Elements of Security Force Effectiveness	**45 Minutes**

Enabling Learning Objective:

- Describe the primary elements that contribute to a security force's effectiveness.

Slide 44 Primary Elements of Security Force Effectiveness
▪ This section will cover: • Selection of security force members • Initial and continuous training • Deployment of equipment • Appropriate supervision
Graphic Description: No Graphic

- Tell participants that the following elements contribute to the effectiveness of a security force:
  - Selection of security force members
  - Initial and continuous training
  - Deployment of adequate equipment
  - Appropriate supervision
- Explain that each will be discussed in detail on the following slides.

Slide 45 Selection of Security Force Members — Pre-Employment

- Background checks
- Medical exams
- Candidate testing and oral interview

Graphic Description: No Graphic

- Tell participants that the first element that contributes to the success of the effectiveness of the security force is selection of force members. Selection begins with initial recruitment and hiring.
- Explain that the following selection criteria should be included in an organization's standard operating procedures manual to help ensure selection of the right candidates. Qualified candidates are chosen based on successfully completion of the following:
  - Pre-employment background investigation check
  - Pre-employment medical examination
  - Candidate testing and oral interview

Slide 46 Selection of Security Force Members — Desirable Qualities (Workbook 12.2)

- Integrity and honesty
- Alertness
- Judgment
- Confidence
- Physical fitness
- Tactfulness
- Self-control

Graphic Description: A group of men exercising for fitness training

- Explain that in addition to pre-employment checks, certain qualities are important for a security force member to possess.
- Refer participants to **Workbook 12.2: Desirable Qualities in Security Force Personnel.**
- Tell participants that these desired qualities in security force personnel are developed through training and become instinctive through experience.

Slide 47 Selection of Security Force Members — Important Considerations

- Mental attitude and quality of job performance are critical
- Assign only the most reliable, responsible, and trustworthy members to the assignments requiring access to sensitive information
- Conduct follow-up investigations to ensure behavior is above reproach

Graphic Description: No Graphic

- Explain that participants should also make these important considerations when selecting security force members:

- Each person's general mental attitude and the quality of job performance are crucial. Only personnel of known responsibility levels and trustworthiness should be assigned to security force duties.
- Security-clearance criteria for security force positions must be based principally on the security classifications of the information to which access will be granted. The reliability, known responsibility levels, and trustworthiness must be evaluated before security force personnel are entrusted with access to classified or sensitive information.
- Follow-up investigations should be conducted on all security force personnel who are granted security clearance to ensure that their actions are above reproach.

Slide 48 Discussion Questions (1 of 2)
▪ What provisions do you have in place to ensure that your critical infrastructure security force or security force remains in good physical condition? ▪ What are the advantages of periodic physical-conditioning assessments and the benefits of a strong, healthy security force? Are there any disadvantages?
Graphic Description: No Graphic

- Ask participants: **What provisions do you have in place to ensure that your critical infrastructure security force or security force remains in good physical condition?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Require security force members to adhere to physical fitness standards, typically in line with military standards.*
  - *Require periodic standards testing to ensure continuous compliance.*
  - *Conduct limited scope performance tests to ensure that security force members are able to perform tactical operations once deployed.*
- Ask participants: **What are the advantages of periodic physical-conditioning assessments and the benefits of a strong, healthy security force? Are there any disadvantages?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Force readiness, increased skill levels, and natural decrease of unfit personnel.*
  - *Disadvantages may include: disinclination to enlist/apply and attrition of skilled strategists who are not within fitness standards.*

Slide 49 Discussion Questions (2 of 2)
▪ What background checks are performed on your security force personnel? ▪ Is it a requirement to conduct periodic background updates, especially for personnel securing critical areas? Why or why not?
Graphic Description: No Graphic

- Ask participants: **What background checks are performed on your security force personnel?**
- Acknowledge responses. *Responses will vary.*

- Ask participants: **Is it a requirement to conduct periodic background updates, especially for personnel securing critical areas? Why or why not?**
- Acknowledge responses. *Responses will vary but may include:*
  - *Security force is very small.*
  - *All members are from the same family or clan.*
  - *There are tight budget restrictions.*

Slide 50 Initial and Continuous Training
▪ Entry-level skills training — various skills ▪ Assignment of coach — ensures recruits gain insight from veteran members ▪ Annual update training — legal updates, new policies, and procedures ▪ Specialized training — dependent upon security force placement
Graphic Description: No Graphic

- Explain that once an organization hires a new security force recruit, the new hire should attend an initial or basic training program that provides the individual with entry-level skills to perform the job.
- Tell participants that training should require successful completion of examinations and practical application.
- Provide examples of entry-level skills courses that might be offered:
  - Firearms
  - Physical fitness
  - Legal requirements
  - Security education and operations
  - Protection of government property
  - Defensive techniques
  - Intermediate force weapons
  - Communications operation
  - Vehicle operations
  - Post and patrol operations
  - Orders, policies, and procedures
  - Awareness of chemical, biological, radiological, and nuclear materials
- Explain that in addition to initial training, a security force recruit should be assigned to a coach or field training officer. This ensures that each recruit gains additional insight into the job from veteran members.
- Explain that beyond basic training and on-the-job training experience, security force members should receive annual update training and specialized training as required.
- Tell participants that annual update training typically consists of any legal updates, new policies and procedures being implemented, or other critical information pertinent to their job function.
- Explain that specialized training will be required depending on the placement on the team. Specialized courses could include the following:
  - Tactical operations training
  - Negotiation training
  - Leadership training

- Instructor development training
- Advanced driver skills training

Slide 51 Deployment of Equipment
▪ Equipment requirements must address security force needs ▪ Inadequate equipment can be detrimental to protecting critical infrastructure
Graphic Description: No Graphic

- Explain that the security force's level of effectiveness is dependent on the resources being supplied. Therefore, equipment requirements must be established to adequately address the security force's needs.
- Explain that a lack of equipment or poorly maintained equipment can be detrimental to protecting a critical infrastructure.
- Provide examples of common deficiencies in equipment:
  - Inappropriate weapons and ammunition
  - Lack of post-maintenance weapons checks
  - Inadequate numbers and types of vehicles
  - Poor vehicle maintenance
  - Insufficient radio frequencies
  - Unreliable radio communications
  - Inadequate personal equipment for duty
  - Inadequate training facilities

Slide 52 Appropriate Supervision
▪ Competent in security force job skills ▪ Experienced in the field ▪ Sufficient number of supervisors ▪ Supervisor development and training
Graphic Description: No Graphic

- Explain that the last primary element contributing to the security force's effectiveness is the type of supervision the security force members receive. A security force supervisor should have the following attributes:
  - Competent in security force job skills
  - Experienced in the field
- Explain that there should be a sufficient number of supervisors to provide appropriate supervision. Establishing a supervisor development program that identifies and selects individuals for the critical role of a supervisor can meet the need.
- Tell participants that in addition to the selection process, supervisors need to be trained in their new role and duties.

Slide 53 Inappropriate Supervision
▪ Common causes: • Lack of qualified, trained, experienced personnel • Poor documentation ▪ Common deficiencies: • Overworked or inattentive supervisors • Lack of coordination with others • Failure to develop emergency tactical skills
Graphic Description: No Graphic

- Explain that the underlying causes of inappropriate supervision of security force members include the following:
  - Lack of qualified, trained, and experienced personnel — the most frequent
  - Issues associated with poor documentation — the second most frequent
- Remind participants that *Module 11: Policies and Procedures* explained the need for documentation that specifies the plans and limits for security force operation under various conditions.
  - These are essential to a supervisor's success.
  - When policies and procedures are applied consistently and appropriately, subordinates have a clear understanding of what is expected and what the outcome could be if the desired results are not achieved.
- Explain that there are other common supervisory deficiencies that have been identified and provide a few of the following examples, or examples from your own personal experiences, as time permits:
  - Inadequate operational supervision
  - Unclear policies defining supervisory responsibilities, which leads to confusion on the part of the supervisor
  - Insufficient number of supervisors, which results in poor span of control
  - Improper operational training of supervisors, which leads to confusion as to the needs of the organization over that of the supervisor or employees
  - Overworked or inattentive supervisors
  - Lack of coordination with other supervisors or superiors
  - Inadequate tactical supervision
  - Lack of appropriate tactical supervisory training
  - Focus on routine responsibilities
  - Failure to develop emergency tactical skills
  - Inadequate post and patrol orders
  - Orders are not updated properly to reflect current practice
  - Large numbers of modifications rather than order re-write
  - Portions of orders may be missing
  - References may refer to outdated orders which supply improper guidance
  - Incomplete or nonexistent response plans or other orders
  - Plans may not be approved by superior departments so lack authority to implement
  - Plans do not include contingency planning elements
  - May contain obsolete information or insufficient detail of information

- Plans do not address support provided by other local agencies

Slide 54 Discussion Questions
▪ In addition to the supervision issues identified, are there any others that you may have experienced? ▪ What tactics could you use to counter these deficiencies or prevent them in the first place?
Graphic Description: No Graphic

- Ask participants**: In addition to the supervision issues identified, are there any others that you may have experienced?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Inadequate records*
  - *Inadequate personnel policies*
  - *Failure to provide adequate supervision*
  - *Lack of management oversight*
  - *Poor communication between security force managers and subordinate supervisors*
- Ask participants**: What tactics could you use to counter these deficiencies or prevent them in the first place?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Improve performance tests*
  - *Increase interdepartmental communication*
  - *Review current training to address specific deficiencies*
  - *Review applicable policies and procedures for currency and relevance*

Topic: Develop a Security Force Response Plan	**15 Minutes**

Enabling Learning Objective:
- Describe the format of a security force response plan.

Slide 55 Develop a Security Force Response Plan
▪ Purpose: to define the processes necessary to enable the security force to successfully accomplish its mission ▪ Content is primarily for emergency response procedures ▪ Plan should be clear, concise, and current
Graphic Description: No Graphic

- Tell participants that knowing the role and function of a security force in the physical protection system and elements of an effective security force helps to create a security response plan brings those aspects together to provide maximum protection of critical infrastructure.
- Explain that the purpose of a security force response plan is to define the processes necessary in the event of an emergency situation to enable the security force to

successfully accomplish its mission of protecting critical infrastructure from theft, sabotage, and other hostile acts — a security force response plan:
  - Provides guidance to the security force when responding to out-of-the ordinary circumstances.
  - Facilitates a rapid, coordinated, appropriate, and successful response to an emergency — insufficient detail or failure to address an important area may result in confusion or an inadequate response.
  - Is not intended for routine daily fixed post or patrol activities — post or patrol orders typically outline activities performed during normal conditions.
  - May be a part of a post or patrol order, referenced as required in the post or patrol order manual.
- Explain that security force response plans include response procedures for a range of emergencies from tactical deployment, evacuations due to bomb threats, and chemical, biological, radiological, and nuclear issues to a direct attack — response plans must ensure that the security force is located in either:
  - Direct defense of asset locations
  - Appropriate ready-response positions that offer immediate access to asset locations
- Explain that security force response plans must be clear, concise, and current and should include required protection strategies, tactical response options, actions, and times.
  - When new information is acquired that would have an effect on the response capabilities of the security force, plans should be updated immediately and, at a minimum, be reviewed by a competent security force authority on an annual basis.
  - If security force response plans affect outside resources such as local law enforcement personnel, appropriate parts of the plan should be shared to ensure that the responding outside agencies understand their roles and responsibilities.
  - When sharing such information, remember that sensitive information is only shared with those with need-to-know privileges.
- Tell participants they will be developing their own security force response plan later in the module.

Slide 56 Security Force Response Plan Format (Workbook 12.3)

- Title
- References
- Definitions and abbreviations
- Purpose
- Guidance
- Reporting requirements

Graphic Description: No Graphic

- Refer participants to **Workbook 12.3: Sample Security Force Response Plan**.
- Explain that the addendum is a sample response plan they will use as a reference when they complete one of their own later during this module. This particular plan gives response procedures for an unauthorized entry of an active shooter in a government facility that is designated as a critical infrastructure.

- Allow participants five minutes to read the addendum.
- Explain that when developing a security force response plan, a simple format should be followed. The following format provides a guide in developing a response plan:
  - **Title** — the plan title and date issued should be on the front cover, additional information may include the specific post or patrol, and the threat the plan was developed to address.
  - **References** — this section provides the title of other documents that relate to the plan; for example, a plan on bomb threats may reference the building evacuation plan for a specific location.
  - **Definitions and abbreviations** — the reader should be able to use this section as a quick reference for terms that may need to be identified or for abbreviations used in the plan.
  - **Purpose** — this section covers the specific area the plan was developed to address and personnel affected by the plan.
  - **Guidance** — this section provides the user with the steps for what to do in the event the plan is to be implemented.
  - **Reporting requirements** — this section identifies the reporting requirements should the plan require implementation.

Slide 57 TeachBack Moment

- What are the primary elements that contribute to the effectiveness of a security force?
- What are the components that should be included in a security force response plan?

Graphic Description: No Graphic

- Conduct a TeachBack moment to assess how well the participants understand the content presented in this section of the module.
- Ask the participants: **What are the primary elements that contribute to the effectiveness of a security force?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Selection of security force members*
  - *Initial and continuous training*
  - *Deployment of adequate equipment*
  - *Appropriate supervision*
- Ask the participants: **What are the components that should be included in a security force response plan?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Title*
  - *References*
  - *Definitions and abbreviations*
  - *Purpose*
  - *Guidance*
  - *Reporting*

Topic: Threaded Exercise Part 5 — National Ministries Building 60 Minutes

Enabling Learning Objective:
- Develop a security force response plan for a given facility.

Slide 58 Threaded Exercise Part 5 — National Ministries Building

- Purpose: to develop a security force response plan
  - Duration: 60 minutes (30-exercise; 20-presentations; 10-debrief)
  - Group composition: table groups
  - Debrief: team presentations; facilitator feedback

Graphic Description: No Graphic

Slide 59 National Ministries Building Complex Map

- *No Text*

Graphic Description: National Ministries Building complex map

- Tell participants that they will apply what they learned in this module to continue the scenario that began in *Module 5: Components of Critical Infrastructure.*
- Refer participants to **Threaded Exercise Part 5 — National Ministries Building** and allow them a few minutes to read the directions.
- Tell participants they will use **Addendum 12.3: Sample Security Force Response Plan** as a resource for this exercise.
- Tell participants that each team will develop a security force response plan for potential threats against the National Ministries Building.
- Assign an interpreter to each team as needed.
- Tell participants that the information they need to develop for their response plan is in **Part 3: Threat Analysis** from *Module 10: Analyzing the Threat*.
- Tell participants may also use any existing plan(s) available in their agency to complete the references section of their plan.
- Tell participants that at this point, cost is not a factor; they can recommend any security force solutions that their team would consider appropriate to prevent or mitigate the threat.
- Emphasize that participants should use their collective judgment (based on personal knowledge or professional expertise) when completing *Table 9: Protest and Demonstration Response Plan Applicability*.
- The teams should be prepared to discuss their security force response plan and explain the rationale used for presenting solutions to the class.
- As participants work, facilitators should walk around the room to answer any participant questions.
- Allow 30 minutes for teams to complete their plans.
- Allow each team 5 minutes to present a summary of their plan.
- Refer to **Threaded Exercise Workbook Part 5 — National Ministries Building Answer Key** for debrief.

- After each team has presented, the facilitator will provide constructive feedback on each plan.

Topic: Module Summary	**10 Minutes**

Slide 60 Module Summary
▪ Relationships between functions ▪ Primary elements of security force effectiveness ▪ Develop a security force response plan
Graphic Description: No Graphic

- Summarize the module by reviewing the following points:
  - **Relationships between functions:**
    - Detection and assessment function
    - Detection function effectiveness
    - Delay function
    - Response function
  - **Primary elements of security force effectiveness:**
    - Selection of security force members
    - Initial and continuous training
    - Deployment of equipment
    - Appropriate supervision
  - **Develop a security force response plan:**
    - Purpose
    - Format
- Ask whether there are any questions about the contents of this module.
- Explain that *Module 13: Security Technology* will explain how to develop a technology plan for the protection of critical infrastructure.