# MODULE 11: POLICIES AND PROCEDURES

**Day**: 5 **Time:** 4.5 Hours **Level of Understanding:** Application

| | |
|---|---|
| Instructional Strategies: | ▪ Lecture<br>▪ Small-Group Discussion<br>▪ Large-Group Discussion<br>▪ Case Study<br>▪ TeachBack Moment |
| Module Equipment/Facilities: | ▪ Standard Classroom Setup<br>▪ Threaded Exercise Workbook Part 4—National Ministries Building Answer Key<br>▪ National Ministries Building Complex Map<br>▪ Handout 11.1: Designating Responsibilities Activity Answer Key |
| Participant Materials/Handouts: | ▪ Workbook 11.1: Policies and Procedures Overview<br>▪ Workbook 11.2: Security Countermeasure Policy and Procedures<br>▪ Workbook 11.3: UN Security Force Operation Policies<br>▪ Reference 11.1: Critical Incident Management Process Phases<br>▪ Handout 11.1: Designating Responsibilities Activity<br>▪ Workbook 11.4: Bomb Threat Management Checklists<br>▪ Threaded Exercise Workbook Part 4—National Ministries Building |

## Terminal Learning Objective

By the end of this module, you will be able to describe the types of policies and procedures needed for the protection of critical infrastructure.

## Introduction

In the previous module, you analyzed the range of potential threats against critical infrastructure. In this module, you will examine ways to help mitigate these threats through the development and implementation of policies and procedures.

Policies and procedures are the first security countermeasure of an effective physical protective system: they apply to **every** aspect of the physical protective system.

Policies and procedures provide guidance to conduct security force operations, deploy security technology, and evaluate the overall effectiveness of your security countermeasures. Without policies and procedures, it would be impossible for security managers to face the range of challenges associated with critical infrastructure security. Think about how vulnerable a facility would be if suddenly all the electronic surveillance equipment failed. How would security personnel respond to maintain the integrity of the facility's security? Policies and procedures provide the guidance that security managers need to respond to situations such as these.

Once you develop your policies and procedures, you must continually review them. Policy and procedure review is a critical step in security planning, particularly as it relates to threats identified in a threat analysis. This review provides security managers with the capability to identify problems before an action occurs and offer insight into how to respond in the event of a terrorist attack.

You may determine that you should implement numerous policies and procedures as part of your response planning. For example, due to the prevalent use of explosives in terrorist attacks, you should consider bomb threat management policies and procedures as part of any effort to protect critical infrastructure. In this module, you will learn to develop a bomb threat management policy for the National Ministries Building in a given scenario. Having a written operational procedure for bomb threats in place may reduce the effect of the threat. The policy will also help to determine the validity or level of the threat and provide a systematic approach to manage the threat.

**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 |
| Policies and Procedures Relating to a Physical Protection System | ▪ Explain how policies and procedures contribute to the overall effectiveness of a physical protection system. | 35 minutes |
| Types of Policies and Procedures to Protect Critical Infrastructure | ▪ Describe the types of policies and procedures required to protect critical infrastructure effectively. | 90 minutes |
| Policies and Procedures Relating to Critical Incidents | ▪ Explain how policies and procedures provide direction and guidance to security personnel during critical incidents. | 40 minutes |
| Bomb Threat Management Plan | ▪ Describe the elements of a bomb threat management policy. | 90 minutes |

| Topic | Enabling Learning Objectives | Approximate Time |
|---|---|---|
| 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 |
|---|---|
| Area lighting | Artificial illumination that exposes locations inside the perimeter that intruders must cross in order to reach their objectives |
| Critical incident | Any natural or man-made event, civil disturbance, or any other occurrence of an unusual or severe nature that threatens to cause or causes the loss of life or injury to citizens or severe damage to property and requires extraordinary measures to protect lives, meet human needs, and achieve recovery |
| Critical incident management plan | A standardized plan that outlines processes and procedures for coordination and control of responses to a terrorist event or natural disaster |
| Incident command post | The location from which the incident commander manages search and response activities |
| Nonmaster key | Unlocks only the lock for which it was made; opposite of a master key that is a single key that unlocks multiple locks |
| Perimeter barrier | A natural boundary, freestanding fence or wall, or the outer walls or divisions of a building |
| Policy | General guidance regarding an organization's operational standards |
| Procedure | A specific series of tasks, steps, and processes necessary to accomplish a particular goal; how the organization intends to carry out operating policies |
| Secure asset | A person, structure, facility, information, material, or process requiring a high level of protection |
| Security policy | A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources |

## Topic: Module Introduction 5 Minutes

### Slide 1 Policies and Procedures

- 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 thoroughly familiar with the sample policy in **Addendum 11.3: UN Security Force Operation Policies** prior to teaching this module to be able to quickly point out examples being discussed during the topic.

### 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 describe the types of policies and procedures needed for the protection of critical infrastructure

*Graphic Description: No Graphic*

- Briefly discuss the terminal learning objective.
- Highlight the key topics to be presented:
  - Policies and Procedures Relating to a Physical Protection System
  - Types of Policies and Procedures to Protect Critical Infrastructure
  - Policies and Procedures Relating to Critical Incidents
  - Bomb Threat Management Plan

### Slide 3 Course Map with VAM Phases

- *No Text*

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

- Show the participants where this module is in relation to the PPS Diagram.
- Explain that Policies and Procedures is the first of the four modules in Phase 3 of the vulnerability analysis methodology and Step 5 in the physical protection system diagram — identify security countermeasures.
- Explain that policies and procedures provide guidelines to ensure employees know what is expected of them and what they can expect in the event of a crisis.

| **Topic: Policies and Procedures Relating to a Physical Protection System** | **35 Minutes** |
|---|---|

Enabling Learning Objective:
- Explain how policies and procedures contribute to the overall effectiveness of a physical protection system.

| **Slide 4 Policies and Procedures Relating to a Physical Protection System** |
|---|
| ▪ This section will cover:<br>• Definitions<br>• Purpose of and need for<br>• Guidelines for writing policies<br>• Characteristics<br>• Updating |
| *Graphic Description: No Graphic* |

- Tell participants that this section will cover policies and procedures:
  - Definitions
  - Purpose of and need for
  - Guidelines for writing policies
  - Characteristics
  - Updating

| **Slide 5 Definitions** |
|---|
| ▪ **Policy:** general guidance regarding an organization's operational standards<br>▪ **Procedure:** a specific series of tasks, steps, and processes necessary to accomplish a particular goal; how the organization intends to carry out operating policies |
| *Graphic Description: No Graphic* |

- Recall the definition of **policies and procedures** from *Module 2: Introduction to Critical Infrastructure Security and Resilience*: basic written guidelines to ensure standard operational physical protection system effectiveness.
- Explain that while usually referred to together, policy and procedure each have a specific definition.
- Define **policy**: general guidance regarding an organization's operational standards.

- Define **procedure**: a specific series of tasks, steps, and processes necessary to accomplish a particular goal; how the organization intends to carry out operating policies.

| **Slide 6 Purposes of Policies and Procedures** |
|---|
| ▪ Establish guidelines for security management<br>▪ Resolve security conflicts or incidents<br>▪ Ensure security of critical infrastructure<br>▪ Important for everyone:<br>• Provide guidance about expectations<br>• Offer a way for settling disputes |
| *Graphic Description: Hand pulling file from a drawer* |

- Explain that that policies and procedures:
  - Establish guidelines for security.
  - Resolve security conflicts.
  - Ensure the security of critical infrastructure.
- Explain that policies and procedures are important because they:
  - Are for everyone in the organization to refer to and ensure employees know what is expected of them and what they can expect.
  - Offer a way of settling most disputes within the organization.

| **Slide 7 Need for Policies and Procedures (1 of 2) (Workbook 11.1)**  |
|---|
| ▪ If actions of employees indicate confusion about conduct<br>▪ If guidance is needed about ways to resolve conflict<br>▪ To comply with governmental policies and laws |
| *Graphic Description: No Graphic* |

| **Slide 8 Need for Policies and Procedures (2 of 2) (Workbook 11.1)**  |
|---|
| ▪ To establish consistent work standards, rules, and regulations<br>▪ To provide consistent security force response<br>▪ To ensure security technologies are functioning properly |
| *Graphic Description: No Graphic* |

- Refer participants to **Workbook 11.1: Job Policies and Procedures Overview,** *Table 1: Policy and Procedure Development Guidelines.*
- Explain the need for policies and procedures using the information in Table 1.
- Explain that some of the reasons policies and procedures are necessary include:
  - If actions of employees indicate confusion about appropriate ways to behave.
  - If guidance is needed about most suitable way to resolve conflict situations.
  - To keep critical infrastructure in compliance with governmental policies and laws.
  - To establish consistent work standards, rules, regulations, code of conduct, and uniform regulations.

  - To provide consistent security force response to situations and incidents.
  - To ensure security technologies are functioning properly and at an appropriate level of security.
- Tell participants that when deciding whether a policy is necessary, any policy developed should meet the needs of the organization, not the specific needs of one poor performing individual.

| **Slide 9 Discussion Question** |
|---|
| ▪ What consequences to critical infrastructure security might result without policies and procedures? |
| *Graphic Description: No Graphic* |

- Ask participants: **What consequences to critical infrastructure security might result without policies and procedures**?
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Failure to provide systematic and standardized training to security force personnel to respond to situations*
  - *Failure to provide adequate testing of security countermeasures*
  - *Failure to provide adequate emergency notification and evacuation response for staff and visitors at a critical infrastructure*
  - *Failure to provide adequately tested and approved security technologies to prevent a terrorist action*
- Explain that failure in any one of the areas discussed would have an effect on the physical protection system. Multiple failures due to a lack of policies and procedures could be catastrophic to security as well as increase costs.
- Tell participants that it often costs more money to fix a problem due to a lack of policies and procedures than the costs to ensure that the policies and procedures are written, enforced, and followed.

| **Slide 10 Guidelines for Writing Policies** |
|---|
| ▪ Determine the goal to accomplish<br>▪ Tell employees why the policy is being implemented<br>▪ Provide clear and specific guidelines<br>▪ Include sufficient detail to effectively communicate the organization's position |
| *Graphic Description: No Graphic* |

- Explain the guidelines for writing policies:
  - Determine the goal to accomplish.
  - Tell employees why the policy is being implemented.
  - Provide clear and specific guidelines.
  - Include sufficient details to effectively communicate the organization's position.
- Tell participants that policies can never provide enough details to address every potential situation.

- Tell participants that sometimes too much information can make the policy difficult to understand.
- Explain the importance of enforcing security policies and ensuring policies and procedures are accurate, current, and consistent.

**Slide 11 Characteristics of Policies and Procedures (1 of 2) (Workbook 11.1)**

- Policies describe organization's standards
- Procedures describe steps to put the standards into action

*Graphic Description: Hand selecting a tabbed file from a drawer*

- Refer participants to **Workbook 11.1: Policies and Procedures,** *Table 2: Characteristics of Policies and Procedures*.
- Explain the difference in characteristics between policies and procedures.
- Explain each policy in the table and the associated procedure presented in Table 2.

**Slide 12 Use-of-Force Policy Example**

- A security force officer must not exceed the amount of force required to stop a subject from carrying out an adversarial action
- A security force officer must, as appropriate, follow the escalation of force continuum as it applies to the situation

*Graphic Description: No Graphic*

**Slide 13 Use-of-Force Procedure Example**

- Security force:
  - Physical restraint
    1. The security force officer, as appropriate, must issue a verbal warning to a subject before taking action.
    2. If a verbal warning is not complied with, the security force officer can then escalate to the use of physical restraint.

*Graphic Description: No Graphic*

- Explain that the slides show an example of a use of force policy and procedure.
- Explain that:
  - The policy of using force provides general guidance for use-of-force, enabling an escalation of the force continuum as it applies to the situation.
  - The procedure gives the specific steps required — for example, the issuance of a verbal warning that is followed by physical restraint if the subject is noncompliant.

**Slide 14 Importance of Updating Policies and Procedures (Workbook 11.1)**

- Vulnerability analysis methodology and risk assessment strategies ensure that the policies and procedures are:

- Accurate
- Current
- Regularly reviewed and revised to meet changing threats

*Graphic Description: No Graphic*

- Explain that the vulnerability analysis methodology and risk assessment strategies are designed to ensure that the policies and procedures of an organization are:
  - Accurate
  - Current
  - Revised as needed to meet changing threats
- Explain that it is important to evaluate policies and procedures on a regular basis to reflect the fact that the risks and vulnerabilities of critical infrastructure may change over time. For example, a policy or procedure written a year ago to address a particular threat may no longer be current if the threat has changed.
- Provide this example to demonstrate the importance of regularly reviewing policies and procedures:
  - Security force officers at a critical infrastructure facility were required to conduct checks on fences surrounding the facility on a scheduled basis within a given timeframe, every 30 minutes.
  - Due to the regularly scheduled patrol, the adversaries conducted surveillance on the fence line patrol and were able to predict the patrol's movements within 5 minutes.
  - This resulted in the adversaries' cutting the fence, gaining entry into a secure area, and stealing valuable equipment.
  - A policy change required unscheduled patrols of the area, and increased patrols at specified hours when there may be a higher probability of an attack on the fence line, such as during nighttime hours.
- Refer participants to **Workbook 11.1: Policies and Procedures,** *Table 3: Policies and Procedures Review.*
- Explain that the table in the addendum provides a summary of policies and procedures that organizations should review regularly to ensure maximum protection of critical infrastructures.
- Tell participants that the next topic will discuss specific types of policy and procedures for protecting critical infrastructure.

## Topic: Types of Policies and Procedures to Protect Critical Infrastructure 90 Minutes

Enabling Learning Objective:

- Describe the types of policies and procedures required to protect critical infrastructure effectively.

**Slide 15 Types of Policies and Procedures to Protect Critical Infrastructure (1 of 2)**

- Develop for:
  - Perimeter barriers
  - Lighting

- Intruder detection systems
- Closed-circuit television
- Automated access control systems
- Security officers and patrols

*Graphic Description: Wall-mounted security camera*

**Slide 16 Types of Policies and Procedures to Protect Critical Infrastructure (2 of 2)**

- Electronic access controls
- Lock and key controls
- Entry control areas
- Secure asset locations
- Cybersecurity

- Include in a standard operating procedures manual

*Graphic Description: No Graphic*

- Explain that the design of security countermeasures for critical infrastructure requires the development of policies and procedures for the following security countermeasures:
  - Perimeter barriers
  - Lighting
  - Intruder detection systems
  - Closed-circuit television
  - Automated access control systems
  - Security officers and patrols
  - Electronic access controls
  - Lock and key controls
  - Entry control areas
  - Secure asset locations
  - Cybersecurity
- Tell participants that organizations should include these policies and procedures in a standard operating procedures manual.
- Tell participants that this section will define, briefly explain, and provide examples of each of these types of security countermeasures.
- Tell participants that *Module 13: Security Technology* will provide more information about how security countermeasures operate.

**Slide 17 Perimeter Barrier Definition**

- Natural boundary, such as a river or mountain range
- Free-standing fence or wall
- Outer walls of a facility or walls or divisions of a building

*Graphic Description: Perimeter fence*

- Define **perimeter barriers**: as a natural boundary, freestanding fence or wall, or the outer walls or divisions of a building.

| **Slide 18 Perimeter Barrier Purpose** |
|---|
| ▪ Delineate a boundary<br>▪ Channel visitors to legal points of entry<br>▪ Deter and delay unlawful intruders<br>▪ Provide a degree of physical, psychological, or legal deterrence |
| *Graphic Description: Protective barriers in front of a government facility* |

- Explain that the purpose of a perimeter barrier is to:
  - Delineate a boundary.
  - Channel visitors to legal points of entry.
  - Deter and delay unlawful intruders.
- Explain that perimeter barriers also provide a degree of physical, psychological, or legal deterrence to intrusion.

| **Slide 19 Perimeter Barrier Effectiveness (1 of 2)** |
|---|
| ▪ Perimeter intruder detection systems<br>▪ Closed-circuit television and security officers<br>▪ Security lighting<br>▪ Enclosed fencing |
| *Graphic Description: Intruder detection system on an access door* |

- Explain that security countermeasures require policies and procedures to help manage and ensure effectiveness.
- Explain that the effectiveness of perimeter barriers can be enhanced by the following methods:
  - Deploying perimeter intruder detection systems
  - Surveillance by closed-circuit television and security officers
  - Security lighting so the area around the barrier remains well-lit during periods of darkness
  - Enclosed fencing around the entire working or operational areas within the facility

| **Slide 20 Perimeter Barrier Effectiveness (2 of 2)** |
|---|
| ▪ Grouped facilities<br>▪ Maintained vegetation<br>▪ Anticlimbing devices on fences<br>▪ Secure vehicle gates and fences at the same level |
| *Graphic Description: No Graphic* |

- Grouping multiple facilities together, when possible, to ensure an efficient and effective means of providing coordinated security. The purpose is to provide the first level of protection to a main facility.
- Maintain the area around the barrier by removing all vegetation (such as grass, weeds, or bushes).
- Anti-climbing devices on fences such as barbed wire outriggers
  - Barbed wire outriggers prevent intruders from successfully climbing over a fence.
  - When a load in the range of 9 to 13 kilos is applied to the outrigger arm, it will break, resulting in the downward movement of the outrigger arm and the fall of the climber.
- If the area is controlled by a vehicle gate(s) allowing access with use of a card reader and monitored by a security officer:
  - Secure the remaining fence perimeter at the same level.
  - Install controlled pedestrian gates or gates that automatically secure when not in use.
  - Install "No Trespassing!" signs to delineate perimeter boundaries and to warn potential trespassers.

**Slide 21 Perimeter Barriers Standards (Workbook 11.2)**

- Doors
- Windows
- Other areas of the facility

*Graphic Description: No Graphic*

- Explain that in addition to the standards for fences, there are standards that should be included in policies and procedures for perimeter barriers such as:
  - Doors
  - Windows
  - Other areas of the facility (including but not limited to roofs, loading docks, public utilities, and air conditioning systems)
- Refer participants to **Workbook 11.2: Security Countermeasure Policy and Procedures, Section 1: Information about Perimeter Barriers**.
- Discuss the standards provided in the addendum tables for each of the areas.

**Slide 22 Lighting (1 of 2)**

- Effective use can minimize the chance that intruders will go undetected

*Graphic Description: Exterior lighting at government building entrance*

**Slide 23 Lighting (2 of 2)**

- All external areas should be well lit:
  - Vehicle parking areas
  - Access routes

- Building entrances
- External doors
- Common entrances

- Use light-sensitive devices for daytime and nighttime conditions

*Graphic Description: No Graphic*

- Explain that lighting is a critical security countermeasure that when used effectively can minimize the chances that intruders will go undetected.
- Tell participants that lighting should cover all areas inside the perimeter that intruders must cross.
- Explain that one policy that must be implemented is to ensure all vulnerable external areas are well lit including:
  - Vehicle parking areas
  - Access routes
  - Building entrances
  - External doors
  - Common entrances
- Tell participants that when installing lighting to illuminate external doors, common entrances, and multi-occupancy buildings, use light-sensitive devices for daytime and nighttime conditions.

**Slide 24 Lighting and Closed-Circuit Television Compatibility**

- Factors that dramatically reduce quality of image include:
  - Excessive shadows
  - Glare into the lens
  - Back-lighting
  - External lighting
- Avoid low-pressure sodium vapor lighting

*Graphic Description: No Graphic*

- Tell participants lighting sources must be compatible with the requirements of closed-circuit television.
- Explain that the following factors will dramatically reduce the quality of images recorded on closed-circuit television:
  - Excessive shadows
  - Glare into the lens
  - Back-lighting
  - External lighting
- Explain that organizations should avoid lighting using low-pressure sodium vapor because these types of lamps only allow detection of movement and do not provide the type of light that is needed for high-quality closed-circuit television images.

**Slide 25 Lighting — Perimeter**

- Should cast a uniform light over the perimeter

| |
|---|
| ▪ Should create a glare that deters intruders (overhead or low-mounted lamp)<br>▪ Should not create a nuisance or hazard outside the perimeter<br>▪ Should not reveal the positions of guards, either inside or outside |
| *Graphic Description: Parking lot lighting* |

- Explain that lighting around the perimeter should cast a uniform light over the perimeter.
- Tell participants about the installation of overhead or low-mounted lamps:
  - Create a glare effect that dazzles and deters intruders.
  - Should not create a nuisance or hazard outside the perimeter.
- Explain that lighting should not reveal the positions of guards:
  - Patrolling outside.
  - Inside security posts or other interior rooms where officers may be seen or detected in silhouette.

| **Slide 26 Lighting — Area** |
|---|
| ▪ Illuminates areas inside the perimeter that intruders must cross in order to reach their objectives and:<br>• Increases security officers' ability to detect intruders<br>• Acts as a powerful deterrent<br>• Should be even and without shadows |
| *Graphic Description: No Graphic* |

- Define **area lighting**: artificial illumination that exposes locations inside the perimeter that intruders must cross in order to reach their objectives.
- Explain that area lighting:
  - Increases the security officers' ability to detect intruders.
  - Acts as a powerful deterrent.
  - Should be even and without shadows.

| **Slide 27 Intruder Detection Systems** |
|---|
| ▪ Designed to:<br>• Detect entry, or attempted entry, of an intruder into a protected area<br>• Identify location of an intrusion<br>• Signal an alarm to the security force<br>▪ Best used to provide early detection of attack<br>▪ Security force must respond quickly |
| *Graphic Description: No Graphic* |

- Explain that intruder detection systems are designed to:
  - Detect the entry, or attempted entry, of an intruder into a protected area.
  - Identify the location of the intrusion.
  - Signal an alarm to security force.

- Explain that an intruder detection system provides early detection of an attack, but does not delay the intruder; it only detects the intruder's presence.
- Tell participants that the policy and procedures should explain:
  - The signal notifying the attack needs to be safely transmitted to a security control center for the security force to initiate immediate action.
  - Security force must react quickly to prevent the intruder from accomplishing the purpose.

**Slide 28 Intruder Detection System Elements**

- Perimeter — activate by intrusion or attack upon the perimeter
- Trap — activate once the intruder is inside the building
- Point — used to protect high-value and portable items

*Graphic Description: No Graphic*

- Explain that an intruder detection system should have a combination of protection that includes:
  - **Perimeter protection** — includes devices activated by intrusion or attack upon the perimeter
  - **Trap protection** — includes devices activated once the intruder is inside the building
  - **Point protection** — includes devices used to protect high value and portable items
- Explain that using a combination of these three approaches is an effective practice to provide the required verification of an incident and to achieve effective and in-depth security, for example: a highly classified document in a point-protected safe that is:
  - Protected inside a facility with intruder trap and a restricted access entry area.
  - Surrounded by a perimeter fence.
  - Protected by sensors and closed-circuit television.
- Tell participants that correctly positioned closed-circuit television cameras will aid in alarm verification.

**Slide 29 Intruder Detection System for Unmanned Facilities (1 of 2)**

- Should be equipped with following features:
  - Door contact sensors, as a minimum requirement
  - Sensors that report to the security control center
  - A security control center that provides access control functions
  - A verification feature that clarifies the reason for alarm activation

*Graphic Description: Door alarm sensor*

- Explain that an intruder detection system for an unmanned facility should have all of the following features listed on the slide.

**Slide 30 Intruder Detection System for Unmanned Facilities (2 of 2)**

- The verification feature can be provided by:

- Closed-circuit television at the remote site
- Law enforcement or security force personnel directed to the site to investigate

- Provides the ability to view the area

*Graphic Description: No Graphic*

- Explain that the verification feature can be provided by:
  - Closed-circuit television at the remote site that is integrated with alarm communication and display to the security control center; this system should be capable of distinguishing a nuisance alarm activation source (vibration from nearby heavy machinery, blowing debris, small animal movement) from an alarm activated by an intruder.
  - Law enforcement or security force personnel directed to the site to investigate the alarm activation source.
- Explain that a verification feature provides the ability to view the area where a sensor was activated, for example: an activated sensor sends an alert to a security officer:
  - The officer views a monitor to determine what or who activated the intrusion detection sensor.
  - The officer responds according to established policies and procedures.

**Slide 31 Closed-Circuit Television (1 of 2) (Workbook 11.2)**

- Benefits include:
  - Saves manpower
  - Makes an existing security system more effective
  - Enhances perimeter security

*Graphic Description: No Graphic*

**Slide 32 Closed-Circuit Television (2 of 2)(Workbook 11.2)**

- Not a security detection device without video motion detection
- Selection of cameras and system based on site requirements

*Graphic Description: No Graphic*

- Refer participants to **Addendum 11.2: Security Countermeasure Policy and Procedures, Section 2: Information about Closed-Circuit Television**.
- Tell participants that another type of policy and procedure to develop is for the use of closed-circuit television.
- Explain that the benefits of closed-circuit television systems include:
  - Saves manpower, especially when used in conjunction with an intruder detection system and automated access control system.
  - Supplements and extends, making an existing security system more effective.
  - Enhances the effectiveness of perimeter security particularly if used to verify the alarms signaled by perimeter intruder detection systems.
- Explain that that closed-circuit television is not a security detection device unless used with video motion detection.

- Explain that selection of closed-circuit television cameras and performance specifications is based on specific site requirements, which must be identified in the design of the physical protection system, for example:
  - General monitoring of large areas is not sufficient to recognize a known individual or vehicle license plate.
  - Identification of an individual or license plate requires increased focal views.
- Tell participants to read the other sections about closed-circuit television presented in the addendum as a reference.
- Tell participants that closed-circuit television technology along with other security countermeasures will be discussed in *Module 13: Security Technology*.

| **Slide 33 Automated Access Control Systems** |
|---|
| ▪ Ensure only authorized persons gain access<br>▪ Minimum requirement: a card-access control system<br>▪ Follow standard operating procedures manual |
| *Graphic Description: Security guard at front gate of government complex* |

- Tell participants that in addition to policies and procedures on perimeter barriers, lighting, intruder detection systems, and closed-circuit television, they must develop policies and procedures for automated access control systems.
- Explain that access to critical infrastructure should be controlled to ensure only authorized persons gain access.
- Tell participants that minimum standard for access control is to use an automated card-access control system.
- Explain that specific access requirements should be identified in the standard operating procedures manual.

| **Slide 34 Automated Access Control Systems — Components** |
|---|
| ▪ Electronic access control<br>▪ Alarm reporting<br>▪ Image capture and badge production<br>▪ Physical locks and key control<br>▪ Alarm output triggers to closed-circuit television system |
| *Graphic Description: No Graphic* |

- Explain that the automated access control system should, at a minimum, incorporate:
  - Electronic access control
  - Alarm reporting
  - Image capture
  - Badge production
- Tell participants that these features should work in conjunction with physical locks and key control to restrict access.

- Explain that the system shall be capable of providing alarm output triggers to the closed-circuit television system. This capability allows for a camera view of the alarm location to be displayed on the spot monitors in the security control center.
- Tell participants that more information about electronic access control and physical locks and key control is provided later in this module.

| **Slide 35 Facility Access Control (1 of 2)** |
|---|
| ▪ Keep number of external access and exit points to a minimum<br>▪ All regular entry and exit points must be access controlled and include anti-pass backup capability |
| *Graphic Description: No Graphic* |

| **Slide 36 Facility Access Control (2 of 2)** |
|---|
| ▪ External doors with remote operation installed where entry is viewed:<br>• Directly<br>• By closed-circuit television<br>▪ Control internal doors leading to critical areas with electronic access |
| *Graphic Description: No Graphic* |

- Tell participants that effective facility access control policies include keeping the number of external access and exit points to a minimum, while still meeting fire safety requirements.
- Define **anti-pass backup capability**: prevents a person from re-entering a secure area unless they follow the appropriate path.
- Explain that other policies ensuring effectiveness include:
  - All regular entry and exit points must be access controlled and have an **anti-pass backup capability**. For example, a person enters a facility through a turnstile that only rotates one way to allow them to enter but does not allow them go back through the turnstile the way they came.
  - Install external doors providing remote access where entry is viewed directly or by closed-circuit television.
  - Control internal doors leading to primary and secondary critical by electronic access control.

| **Slide 37 Security Officers and Patrols (1 of 2)** |
|---|
| ▪ Where applicable, lead security officer determines security level policies and procedures based on:<br>• Informed opinions on threats<br>• Specific vulnerabilities<br>• Identified risks |
| *Graphic Description: No Graphic* |

**Slide 38 Security Officers and Patrols (2 of 2)**

- Integrate security measures into one security control center facility protecting:
  - Security personnel
  - Reception staff
  - Systems data

*Graphic Description: Security officer viewing closed-circuit video monitors*

- Explain that the need to develop policies and procedures regarding security officers and patrols.
  - Where applicable, the lead security officer (for example, the Chief of Security) determines security level policies and procedures. The lead security officer should base decisions on:
    - Informed opinions from local, country, and government threats
    - Specific vulnerabilities
    - Identified risks and their likelihood of occurring or being exploited
- Security measures should be fully integrated into one security control center facility. The security control center facility should provide the maximum protection for the:
  - Security personnel
  - Reception staff
  - Systems data

**Slide 39 Electronic Access Control**

- Requires specific policies and procedures
- Examples include:
  - Specific management responsibilities for card control and inventory requirements
  - Guidelines for issuing cards and the areas to be granted access
  - Guidelines for terminating card access for misuse of cards

*Graphic Description: No Graphic*

- Tell participants that electronic access control requires specific policies and procedures, for example:
  - Specific management responsibilities for card control and inventory requirements.
  - Guidelines for issuing cards and the areas to be granted access.
  - Guidelines for terminating card access for misuse of cards.
- Explain that electronic access control units are increasingly being used, but lock and key units are still used.

**Slide 40 Lock and Key Controls (Workbook 11.2)**

- Standards
- Spare keys
- Key labeling

*Graphic Description: No Graphic*

- Refer participants to **Addendum 11.2: Security Countermeasure Policy and Procedures, Section 3: Information about Lock and Key Controls**.
- Briefly discuss the material in the addendum covering the three areas to consider when developing policies and procedures for lock and key controls.
- Briefly discuss the three sections in the addendum concerning lock and key controls:
  - Standards
  - Spare keys
  - Key labeling

| **Slide 41 Entry Control Areas — Personnel** |
|---|
| ▪ All personnel must wear a visible identification card<br>▪ Revoke access when a staff member leaves the organization<br>▪ Verify and authorize access for any external support services personnel |
| *Graphic Description: Examples of two badges from same person* |

- Explain that basic minimum requirements for personnel entry into a vital infrastructure should include:
  - All personnel must be issued an identification card that must be visibly worn while on the facility.
  - Access rights to work areas must be revoked immediately for any member of staff who leaves the organization.
  - Access by any external support services personnel must be verified and authorized.

| **Slide 42 Entry Control Areas — Visitors** |
|---|
| ▪ Ask person they are visiting to arrange access<br>▪ Obtain permission prior to the day of visit<br>▪ Be issued an identification card<br>▪ Obtain a visitor card at reception desk<br>▪ Be accompanied by an authorized person at all times |
| *Graphic Description: No Graphic* |

- Explain the basic minimum requirements for visitor entry into a critical infrastructure. Visitors should:
  - Ask person they are visiting to arrange access.
  - Be required to obtain permission prior to the day of the visit.
  - Be issued an identification card.
  - Obtain a visitor card at the reception desk.
  - Be accompanied at all times by an authorized person.
- Tell participants that access must only be granted for specific purposes and employees must challenge unaccompanied strangers or anyone not wearing an identification card or pass in the workplace.

| Slide 43 Secure Asset Locations (1 of 2) |
|---|
| ▪ Locate in interior of facility<br>▪ Keep away from exterior windows<br>▪ Do not use glass doors or windows for construction<br>▪ Use metal or solid wood doors<br>▪ Control access using electronic access control with capability to maintain a record of all entrants |
| *Graphic Description: No Graphic* |

- Define **secure asset:** a person, structure, facility, information, material, or process requiring a high level of protection.
- Explain the requirements for secure asset locations:
  - If practical, restricted spaces should be located in the interior of the facility and away from exterior windows.
  - If possible, secure asset areas should not have glass doors or windows.
  - Metal-clad doors or solid wood doors should be used at all restricted space entrances.
  - Entrance to the secure asset areas should be by means of electronic access control with the capability to maintain a record of all entrants.

| Slide 44 Secure Asset Locations (2 of 2) |
|---|
| ▪ Remove exterior room door key access hardware from the master key system<br>▪ Control issuance of nonmaster keys<br>▪ Install intruder detection system with uninterrupted power source<br>▪ Do not include on floorplans and construct slab-to-slab |
| *Graphic Description: Key with blank label on key ring* |

- Define **nonmaster key:** unlocks only the lock for which it was made; opposite of a master key that is a single key that unlocks multiple locks.
- Explain further requirements for secure asset locations:
  - Remove exterior room door hardware that has key access from the master key system of the facility; convert those keys to nonmaster keys with restricted issuance.
  - Control nonmaster keys by issuing only to individuals with an ongoing business need.
  - Install an intruder detection system on all secure asset locations. The access control and intruder detection systems should have an uninterrupted power supply backup.
  - Do not include the location of critical assets on any floor plan that might be considered general use. Construction of restricted space should be slab-to-slab and adhere to construction requirements.

| Slide 45 Secure Asset Locations — Personnel |
|---|
| ▪ Only personnel with an ongoing business need should be given unescorted access |

| |
|---|
| ▪ Remove names from card access system immediately when no longer required<br>▪ Keep visitors to a minimum |
| *Graphic Description: No Graphic* |

- Explain that:
  - Only personnel having an ongoing recurring business need should be given unescorted access to the secure asset areas.
  - If access is no longer required, the individual's name should be removed immediately from the card access system.
  - Visitors should be kept to a minimum, with tours conducted by authorized personnel.

| **Slide 46 Security Personnel** |
|---|
| ▪ Control access<br>▪ Conduct building searches<br>▪ Perform patrol duties<br>▪ Use the radio to communicate<br>▪ Respond to an intrusion alarm |
| *Graphic Description: No Graphic* |

- Explain the types of procedures important to security personnel.
  - Control access
  - Conduct building searches
  - Perform patrol duties
  - Use the radio to communicate
  - Respond to an intrusion alarm
- Tell participants that procedures provide security personnel with the **what** and the **how** to perform their duties.
  - Nearly every aspect of their position requires them to respond in a specified manner.
  - Without adequate documented procedures, in conjunction with hands-on training and real life experience, it would be difficult for security personnel to meet the challenges they face on the job.
- Provide an example, such as:
  - A security force member is assigned to a main vehicle gate to a critical infrastructure. He opens his standard operating procedures manual to review his responsibilities. The procedures he will follow for the day provide instruction on how to:
    - Check a driver's identification and respond in the event the driver presents false credentials.
    - Conduct a vehicle search of commercial vehicles coming into the critical infrastructure secure area.
    - Properly identify and record a visitor's information before allowing them to enter the critical infrastructure secure area.

    - Respond in the event an explosive device is found on a vehicle attempting to enter the critical infrastructure secure area.
    - Secure the vehicle gate once his shift has ended and the gate is closed for a specified time.
- Tell participants that on the next slides they will review an excerpt from a policy and procedure manual and discuss types of policies to include.

**Slide 47 Types of Policies in a Standard Operating Procedures Manual (Workbook 11.3)**

- Description of the facility site
- Floor plan of the facility
- Description and application of access controls for the facility
- Security force responsibilities

*Graphic Description: No Graphic*

- Refer participants to **Workbook 11.3: UN Security Force Operation Policies.**
- Explain that this addendum contains information about types of policies and provides and an excerpt of the policies and procedures for security force operations by the United Nations.
- Use the addendum to discuss the following policies that the manual should include:
    - A description of the facility site.
    - The floor plan of the facility.
    - The description and application of access controls for the facility.
    - The security force responsibilities.
- Tell participants that you will direct them to specific procedure examples for two of the policies in the addendum as a reference throughout this discussion on types of policies.
- Refer to the **Closed-Circuit Television Procedures Example** (page 13) in the addendum and expand on this policy by adding the following procedures example that provides steps to ensure that the policy is effectively managed:
    - Security officer will sign a site log which contains Officer Name, Time and Date, Signature
    - Closed-circuit television system must be reviewed each day by playing back 15 seconds of recording for each camera to ensure camera is:
        - Functioning
        - Play back is clear
        - Camera is properly positioned
    - Deficiencies will be noted and reported to site supervisor
- Refer to the **Security Incident Involving Guards section** (page 16) in the addendum and expand on this policy by providing the following security incident procedures example:
    - Security officer in violation will be escorted to site supervisor's office; weapon will be removed prior to entering supervisor's office
    - Once site supervisor has briefed the guard, the guard will be escorted from the site
    - The security officer's company ID badge will be confiscated by site supervisor

  - Security officer will be removed from both electronic and manual access entry systems
  - Each shift supervisor will be advised of incident and suspension and make such information available to their shift guards
- Explain that all policies and procedures should be documented in a standard operating procedures manual to provide direction and help ensure consistency in performance.
- Tell participants that organizations that possess a security force should have a wide range of policies and procedures.
- Discuss other examples of policies and subsequent procedures as listed in the addendum and from the UN policy as time permits.

**Slide 48 Policies and Standardized Operational Procedures (1 of 2) (Workbook 11.3)**

- Outline roles and responsibilities of response force personnel
- Reflect general requirements of the lead security officer

*Graphic Description: No Graphic*

**Slide 49 Policies and Standardized Operational Procedures (2 of 2) (Workbook 11.3)**

- Are reviewed annually with updates completed in a timely manner
- Provide guidance on how and when to deploy specialized units

*Graphic Description: No Graphic*

- Explain that policies and standardized operational procedures should:
  - Outline the roles and responsibilities of the response force personnel.
  - Reflect the general requirements as directed by the lead security officer.
  - Be reviewed annually and updates should be completed in a timely manner.
  - Provide guidance on how and when to deploy specialized units.
- Refer participants to **Workbook 11.3: UN Security Force Operation Policies,** to discuss examples of policies and procedures meeting the characteristics on the slide.

**Slide 50 Effective Security Policies (Workbook 11.3)**

- Simple introduction and purpose
- Policy statement
- Information about:
  - Compliance measurement
  - Sanctions for compliance failures

*Graphic Description: Employee using checklist on a clipboard*

- Define **security policy:** a set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.
- Explain that an effective security policy includes:
  - A simple introduction that conveys the purpose of the policy.

- The policy statement itself.
- Information about how compliance will be measured and information about what sanctions will be taken against those that fail to comply.
- Guidelines for the development of a compliance program.

- Refer participants to **Workbook 11.3: UN Security Force Operation Policies,** to discuss examples of security policies in the addendum.

**Slide 51 Noncompliance of Policies and Procedures (Workbook 11.3)**

- If a facility fails an audit or inspection, sanctions can range from:
  - Development of a corrective action plan
  - Closure of the facility until the compliance issue is corrected

*Graphic Description: No Graphic*

- Refer participants to **Workbook 11.3: UN Security Force Operation Policies** to discuss noncompliance.
- Explain the question regarding the completeness of policies and procedures rarely becomes an issue unless the critical infrastructure fails an audit or does not meet all the requirements of the inspection. If a facility does fail an inspection, the sanctions can range from:
  - The development of a corrective action plan
  - Closing down the facility until the compliance issue(s) can be corrected
- Tell participants that because several national agencies may require compliance to specific laws, regulations, and other directives, compliance measurement may be difficult to determine.

**Slide 52 Development of a Compliance Program (1 of 2) (Workbook 11.3)**

- Identify agency that possesses jurisdiction
- Obtain data from past inspections and audits
- Develop a self-audit plan
- Conduct a self-assessment against criteria published

*Graphic Description: No Graphic*

**Slide 53 Development of a Compliance Program (2 of 2) (Workbook 11.3)**

- Develop an action plan
- Incorporate compliance measures from past audits

*Graphic Description: No Graphic*

- Refer participants to **Workbook 11.3: UN Security Force Operation Policies** to discuss compliance.
- Tell participants that a few general guidelines on developing a compliance program include to:
  - Identify the agency that possesses jurisdiction on the issue.

  - Obtain any pertinent data from past inspections or audits to see how the agency conducts such inquiries.
  - Develop a self-audit plan that will at least provide a baseline for the issues the agency may be reviewing.
  - Conduct a self-assessment or audit against the criteria established by the agency.
  - Develop an action plan, if necessary, to take corrective actions; or determine before the next agency inspection why compliance was not met and if it will be met.
- Explain that depending on the type of audit and the specific compliance measures observed from past critical infrastructure, your compliance program should also include:
  - Testing of security technology to ensure operability.
  - Evaluating security force response to a critical infrastructure location (*Module 12: Security Force Operations* will discuss this in greater detail).
  - Reviewing the threat analysis statement to ensure updated intelligence has been included (*Module 10: Analyzing the Threat* covered the threat analysis statement).
  - Assessing security force management's ability to guide and direct security personnel and allied groups during a critical incident (*Module 12: Security Force Operations* will discuss this in greater detail).
- Provide an example:
  - The US Department of Energy facility failed to meet the compliance requirement for Security Awareness Training for all staff and contractor personnel.
    - The issue was noted in the previous inspection, the year before.
    - When the facility failed the inspection again, senior management at the headquarters building in Washington, DC, decided that facility management was not taking security seriously.
    - They decided to cancel all official travel, vacations, and other work.
    - The facility was not able to conduct business as usual until compliance was met.
    - In this case, compliance was stated as: "All employees and contractors of the US Department of Energy must attend an 8 hour Security Awareness Training program and pass a final examination. Compliance must be 100% of the personnel to accomplish this directive."

**Slide 54 TeachBack Moment**

- What types of policies and procedures are needed to effectively protect critical infrastructure?
- What types of policies should be included in a standard operating procedures manual?

*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 types of policies and procedures are needed to effectively protect critical infrastructure?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Perimeter barriers*

- *Lighting*
- *Intruder detection systems*
- *Closed-circuit television*
- *Automated access control systems*
- *Security officers and patrols*
- *Electronic access controls*
- *Lock and key controls*
- *Entry control areas*
- *Secure asset locations*
- *Cybersecurity*

- Ask participants: **What types of policies should be included in a standard operating procedures manual?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Description of the facility site*
  - *Floor plan of the facility*
  - *Description and application of access controls for the facility*
  - *Security force responsibilities*

| **Topic: Policies and Procedures Relating to Critical Incidents** | **40 Minutes** |
|---|---|

Enabling Learning Objective:

- Explain how policies and procedures provide direction and guidance to security personnel during critical incidents.

| **Slide 55 Policies and Procedures Relating to Critical Incidents** |
|---|
| ▪ This section will cover:<br>• Critical incident definition<br>• Critical incident management plan<br>• Critical incident management plan process |
| *Graphic Description: No Graphic* |

- Tell participants this section of the module will discuss how policies and procedures relate to critical incidents.

| **Slide 56 Critical Incident Definition** |
|---|
| ▪ An event of unusual or severe nature that can cause:<br>• Loss of life or injury to citizens<br>• Damage to property<br>▪ Critical incidents require extraordinary measures to protect lives and restore order<br>▪ Policies and procedures provide guidance for effective response |
| *Graphic Description: No Graphic* |

- Tell participants that now that they understand the types of policies and procedures to include in their standard operating procedures manual, they must focus on how to provide security personnel with the guidance they need to respond to critical incidents effectively.
- Define **critical incident**: any natural or man-made event, civil disturbance or any other occurrence of an unusual or severe nature that threatens to cause or causes the loss of life or injury to citizens or severe damage to property and requires extraordinary measures to protect lives, meet human needs, and achieve recovery.[1]
- Tell participants that during times of critical incidents, it requires extraordinary measures to protect lives and restore order.
- Explain that terrorist attacks are typically critical incidents because they are purposely designed to inflict harm, cause destruction, and require extraordinary means to resolve.
- Explain that this section is not intended to teach participants how to manage critical incidents, but rather how to ensure that policies and procedures provide the necessary guidance for security personal to effectively respond to certain incidents.

| **Slide 57 Discussion Questions** |
|---|
| ▪ What are some examples of critical incidents?<br>▪ What are some specific examples of critical incidents in your region? |
| *Graphic Description: No Graphic* |

- Ask participants: **What are some examples of critical incidents?**
- Acknowledge response: *If not provided by participants, add the following:*
  - *Natural disasters*
  - *Hostage situations*
  - *Civil disorder*
  - *Large-scale demonstrations*
  - *Terrorist attacks*
- Ask participants: **What are some specific examples of critical incidents in your region?**
- Acknowledge responses. *Reponses will vary.*

| **Slide 58 Critical Incident Management Plan** |
|---|
| ▪ A standardized plan that outlines processes and procedures for coordination and control of responses to a terrorism event or natural disaster |
| *Graphic Description: Coordination meeting for critical incident planning* |

[1] The United States Federal Emergency Management Agency

- Define **critical incident management plan**: a standardized plan that outlines processes and procedures for coordination and control of responses to a terrorism event or natural disaster.

| **Slide 59 Discussion Questions** |
|---|
| ▪ Does your agency have a critical incident management plan?<br>▪ If so, how does the plan work? |
| *Graphic Description: No Graphic* |

- Ask participants the following discussion questions: **Does your agency have a critical incident management plan? If so, how does the plan work?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Involves all responding agencies, private organizations, and nongovernmental organizations in planning, training, and exercise activities*
  - *Integrates the incident command system into our jurisdiction's emergency operations center and procedures*
  - *Coordinates the sharing of information and intelligence between the incident command post and the emergency operations center or other multiagency coordination entity*
  - *Identifies, mobilizes, dispatches, tracks, and recovers incident resources*
  - *Establishes a joint information system to coordinate the release of information to the public*
  - *Conducts joint training exercises*
  - *Prepares after-action reports based on joint training exercise response performance and actual real-world incident performance*
- Explain that it is important that nations prepare for possible natural disasters, terrorist attacks, and other critical incidents by establishing and implementing a standardized critical incident management plan.
- Tell participants that an effective critical incident management plan outlines processes and procedures for coordination and control of responses to a natural disaster, terrorist threat, attack or other critical incident; this process will be discussed on the next slides.

| **Slide 60 Principles of the Critical Incident Management Process (1 of 2)** |
|---|
| ▪ Must be applied before, during, and after any incident<br>▪ May require multiple jurisdiction and cross-functional agency involvement<br>▪ Various responders must operate under the principles of flexibility and standardization to effectively function as a unified team |
| *Graphic Description: Two arrows labeled Flexibility and Standardization, one above and one below a line* |

- Explain the principles of the critical incident management process:
  - The process-oriented approach to critical incident management rests on working principles that must be applied before, during, and after any incident.

- Most incidents are managed on a daily basis by a single jurisdiction at the local level.
  - Some successful domestic incident management operations depend on the involvement of multiple jurisdictions, functional agencies, and emergency responder disciplines.
  - Critical incidents like terrorist attacks and natural disasters require multiple jurisdiction and cross-functional agency involvement.
  - Tell participants that in order for this broad spectrum of responders to function effectively as a unified team, they must operate under the principles of flexibility and standardization.
  - Explain that a unified team includes security, facilities, and maintenance personnel along with any other persons needed to have a successful resolution.

**Slide 61 Principles of the Critical Incident Management Process (2 of 2)**

- The process provides:
  - Consistent, flexible, and adjustable national framework of government and private entities working together to manage domestic incidents
  - Standardized organizational structures:
    - Incident command system
    - Multiagency coordination systems
    - Public emergency communication systems

*Graphic Description: No Graphic*

- Explain that the critical incident management process provides:
  - A consistent, flexible, and adjustable national framework.
    - Government and private entities at all levels can work together to manage domestic incidents, regardless of their cause, size, location, or complexity.
    - Flexibility applies across all phases of incident management: prevention, preparedness, response, and recovery.
  - A set of standardized organizational structures, for example:
    - An incident command system.
    - Multiagency coordination systems.
    - Public emergency communication systems.
- Tell participants that, due to the number of organizations and agencies involved in the critical incident management process, flexibility and standardization are extremely important to critical incident management success.

**Slide 62 Components of the Critical Incident Management Process**

- Command and management structure
- Joint operations
- Resource and policy
- Communications and information
- After-actions reporting
- Joint training exercises

*Graphic Description: No Graphic*

- Explain that critical incident management process provides requirements for processes, procedures, and systems designed to improve interoperability among jurisdictions and disciplines across these six components:
  - Command and management structure
  - Joint operations
  - Resource and policy management
  - Communications and information management
  - After-action reporting
  - Joint training exercises

**Slide 63 Critical Incident Management Process Phases (Reference 11.4)**

1. Prevention
2. Preparedness
3. Response
4. Recovery

*Graphic Description: No Graphic*

- Explain that effective critical incident management plans address all four phases of the critical incident management process.
- Explain that this process is a cycle that reoccurs with each critical incident.
- **Reference 11.1: Critical Incident Management Process Phases** provides the participants with more information on each phase.

**Topic: Bomb Threat Management Plan** **90 Minutes**

Enabling Learning Objective:
- Describe the elements of a bomb threat management policy.

**Slide 64 Bomb Threat Management Plan (1 of 2)**

- This section will cover:
  - Step 1: Designate management responsibilities
  - Step 2: Define procedures for handling bomb threat calls
  - Step 3: Determine procedures for evaluating bomb threat calls

*Graphic Description: No Graphic*

**Slide 65 Bomb Threat Management Plan (2 of 2)**

- Step 4: Identify an incident command post
- Step 5: Develop a search and evacuation plan
- Step 6: Establish a response procedure

*Graphic Description: Incident commander pointing to a situation board*

- Explain that although there are numerous policies and procedures that should be implemented to manage critical incidents, because of the prevalence of terrorist attacks involving the use of explosives, the final focus for this module is on bomb threat management.
- Tell participants that to help them develop an effective bomb threat management policy, this section will cover the following steps:
  - Step 1: Designate management responsibilities
  - Step 2: Define procedures for handling bomb threat calls
  - Step 3: Determine procedures for evaluating bomb threat calls
  - Step 4: Identify an incident command post
  - Step 5: Develop a search and evacuation plan
  - Step 6: Establish a response procedure

**Slide 66 Discussion Questions**

- Does your agency have a bomb threat management plan?
- If you have one, how does it work?
- What benefits and deficiencies do you notice?
- If your agency does not have one, how do you see one being helpful?

*Graphic Description: No Graphic*

- Ask participants: **Does your agency have a bomb threat management plan?**
- Acknowledge responses. *Responses will vary.*
- Ask participants: **If you have one, how does it work?**
- Acknowledge responses. *Responses will vary.*
- Ask participants: **What benefits and deficiencies do you notice?**
- Acknowledge responses. *Responses will vary.*
- Ask participants: **If your agency does not have one, how do you see one being helpful?**
- Acknowledge responses. *Responses will vary.*

**Slide 67 Step 1: Designate Management Responsibilities (1 of 4)**

- Incident commander:
  - Assess threat calls
  - Order evaluation
  - Supervise search and response to suspect objects
  - Determine when facility can be reentered
- Alternate incident commander:
  - Notify all operations supervisors of bomb threat
  - Direct supervisors to initiate the response procedures

*Graphic Description: No Graphic*

- Explain that the step 1 in developing a bomb threat management plan at a critical infrastructure facility involves the assignment of roles and responsibilities for each role, should a threat occur.

- Explain that this process begins with the assignment of the incident commander — in most cases, the senior security or safety manager should be designated as the incident commander.
- Explain the incident commander's responsibilities listed on the slide:
  - Assessing threat calls and evaluating the origin of the threat.
  - Supervising search activities and ordering necessary evacuations.
  - Supervising responses to any suspect objects, and determining when it is safe for personnel to re-enter the facility.
- Tell participants that an alternative incident commander should be designated — this person assumes the role of incident commander during the incident commander's absence or at the incident commander's discretion.
- Explain the alternate incident commander's responsibilities listed on the slide:
  - Notify all operations supervisors that a bomb threat exists.
  - Direct supervisors or floor wardens to initiate the response procedure.

**Slide 68 Step 1: Designate Management Responsibilities (2 of 4)**

- Supervisor or floor warden:
  - Notify employees of threat
  - Supervise search or evacuation activities
- Runner:
  - Notify supervisors and management about threat
  - Assist in securing location of suspect objects
  - Assign one to each shift to help with miscellaneous needs
- Personnel who answer outside phone lines
- Security and maintenance personnel assigned to search teams

*Graphic Description: No Graphic*

- Explain the responsibilities of the operation's **supervisor or floor warden** listed on the slide:
  - Notifies employees of the threat.
  - Then supervises any search or evacuation activities.
- Explain that a **runner** is designated to aid the incident commander in managing the various activities required to control bomb threat response.
- Explain the responsibilities of the runner listed on the slide:
  - Notify supervisors and management about the threat, and hand-relaying messages.
  - Assist in securing the location of any suspect objects while waiting for law enforcement to arrive.
  - Miscellaneous needs (such as receiving arriving law enforcement or unlocking gates for emergency responders).
- Tell participants that at least one runner and one alternate runner should be designated for each working shift.
- Explain that all receptionists or employees that answer publicly listed telephone numbers should be trained in the proper procedures for talking to callers that are making bomb threats.
- Explain that security and maintenance personnel should be tasked with:

- Being part of the search teams.
- Searching high-priority locations.
- Searching areas that are not covered by a floor warden's zone.

**Slide 69 Step 1: Designate Management Responsibilities (3 of 4) (Handout 11.1)**

- Purpose: to identify the basic roles and responsibilities of the personnel who are responsible for managing a bomb threat incident
  - Duration: 15 minutes (10-activity; 5-debrief)
  - Group composition: table groups
  - Debrief: large-group discussion

*Graphic Description: No Graphic*

- Explain that step 1 in developing a bomb threat management plan at a critical infrastructure facility involves the assignment of roles and responsibilities for each role, should a threat occur.
- Explain that this process begins with the assignment of the incident commander — in most cases, the senior security or safety manager should be designated as the incident commander.
- Refer participants to **Handout 11.1: Designating Responsibilities Activity**.
- Explain that the purpose of the activity is to identify the basic roles and responsibilities of the personnel who are responsible for managing a bomb threat incident.
- Tell participants to work in their table groups to complete the table in the addendum, listing roles and responsibilities for each of the personnel.
- Allow 10 minutes for the activity and 5 minutes for the debrief.
- Conduct a large-group discussion asking teams to share their responses to debrief the activity.

**Slide 70 Step 1: Designate Management Responsibilities (4 of 4)**

- Communications network:
  - Established through the chain of command
  - Ensures employees are properly informed and supervised
  - Mirrors existing management structure
  - Ensures everyone is aware of their role
  - Described when policy is developed

*Graphic Description: Top down view of person typing on a keyboard and a monitor*

- Explain that a communications network:
  - Should be established through the organization's chain of command
  - Ensures that employees are properly informed and supervised while responding to the threat
  - Works best if it mirrors the organization's existing management structure
  - Ensures all parties are aware of their role
  - Should be completely described in writing at the time the policy is developed

**Slide 71 Step 2: Define Procedures for Bomb Threat Calls (1 of 3) (Workbook 11.4)**

- Remain calm
- Listen carefully to the caller's message
- Ask the caller to repeat the message
- Record or write down every word the caller says

*Graphic Description: No Graphic*

**Slide 72 Step 2: Define Procedures for Bomb Threat Calls (2 of 2) (Addendum 11.4)**

- Try to convince the caller to provide:
  - Location of the device
  - Time of detonation
- Ask someone else to listen to the call
- Keep the caller on phone as long as possible

*Graphic Description: No Graphic*

**Slide 73 Step 2: Define Procedures for Bomb Threat Calls (2 of 2) (Addendum 11.4)**

- Pay special attention to:
  - The sound of the caller's voice
  - The caller's dialect or use of language
  - Background noises
- Immediately report the situation to security
- Complete a bomb threat checklist

*Graphic Description: No Graphic*

- Explain that Step 2 establishes policies and procedures to be put in place to manage bomb threat phone calls that will help anyone answering the telephone know what to do if they receive a bomb threat.
  - Bomb threats may come in many forms such as email, letters, or from an informant, but the most common threat will be by phone.
  - Policies and procedures must also be in place for managing the other types of communication, although this addendum focuses on phone threats.
- Refer participants to **Workbook 11.4: Bomb Threat Management Checklists,** *Table 1: Bomb Threat Checklist*.
- Tell participants that this checklist should be used any time a bomb threat is received.
- Explain the policy for managing bomb threats: All bomb threats affecting the facility shall be recorded and reported immediately.
- Explain the procedure for managing bomb threat calls:
  - When a threat call arrives, the person receiving the call should remain calm.
  - Listen carefully to the caller's message.
  - Ask the caller to repeat the message.

- Record or write down every word the caller says.
- At a minimum, the recipient should try to convince the caller to provide two critical facts:
  - Location of the device
  - Time of detonation
- Signal someone else in the room to come and listen in on the call.
  - Many people are shocked when they receive a bomb threat and often overlook small details of the caller's statements.
  - Two people will have a much better chance of remembering the specific details of a call than one person alone.
- Keep the caller on the line as long as possible.
  - Ask the caller specific questions such as what type of device, what it looks like, why the caller placed the bomb, and who the caller is.
  - Tell the caller that the facility is occupied and that a detonation may result in the death or injury of innocent people.
  - The objective is to gain as much information as possible about the caller and the credibility of the threat.
  - If the recipient is in doubt about what to ask, they should refer to the bomb threat checklist for a list of questions.

- Explain that while listening to the caller, the recipient should pay special attention to sounds. For example:
  - The sound of the caller's voice
  - The caller's use of idiom (a language, dialect, or style of speaking that may identify the caller as belonging to a certain group of people or a certain location)
  - Noises in the background
  - Any other indications of the caller's identity or the source of the call
- After the caller hangs up, immediately report the situation to the incident commander or a security officer.
  - Before speaking with anyone else, the recipient should complete the questions on the bomb threat checklist.
  - This ensures proper documentation of the threat while everything is fresh in the recipient's mind.

| **Slide 74 Step 2: Bomb Threat Calls Discussion** |
|---|
| ▪ What existing procedures do you have in place in your agency for managing bomb threat calls? |
| *Graphic Description: No Graphic* |

- Ask participants: **What existing procedures do you have in place in your agency for managing bomb threat calls?**
- Acknowledge responses. *Responses will vary.*

| Slide 75 Step 3: Determine Procedures for Evaluating Bomb Threat Calls |
|---|
| ▪ Once the threat call is received and security is notified, the incident commander should:<br>• Debrief the person who received the call<br>• Let the recipient of the call describe the conversation in his or her own words<br>• Review the completed bomb threat checklist |
| *Graphic Description: No Graphic* |

- Explain that Step 3 is determining a procedure for evaluating threats and deciding on the next course of action.
- Tell participants that once the threat call is received and security is notified, the incident commander should:
  - Debrief the person who received the call.
  - Let the call recipient describe the conversation in his or her own words to help ensure that the recipient is speaking directly from memory without the influence of outside suggestions.
  - Review the completed bomb threat checklist to ensure that the person recorded every detail to the best of his or her ability.

| Slide 76 How to Determine the Authenticity of a Bomb Threat |
|---|
| ▪ Authentic bombers tend to:<br>• Repeat the threat message in a specific manner<br>• Provide detailed descriptions about the location of the device<br>▪ The more information provided, the more likely threat is real |
| *Graphic Description: No Graphic* |

- Explain that authentic bombers tend to:
  - Repeat their messages in a specific manner
  - Provide detailed descriptions of the location of the device
- Tell participants that the more information provided by the caller, the greater the chances are that the call is real.

| Slide 77 Bomb Threat Decision Options (1 of 2) |
|---|
| ▪ Evacuate<br>▪ Search<br>▪ Ignore the threat<br>▪ Do not base decisions solely on threat call's credibility |
| *Graphic Description: No Graphic* |

| **Slide 78 Bomb Threat Decision Options (2 of 2)** |
|---|
| ▪ The option chosen should be made in accordance with the bomb threat management plan<br>▪ Guidelines for decisions about search and evacuation should be established by policy |
| *Graphic Description: No Graphic* |

- Explain that a decision needs to be made about whether to:
  - Evacuate
  - Search
  - Ignore the threat
- Explain that an organization should not make this decision on the basis of the call's credibility, but according to standard protocols defined in the bomb threat management plan, for example:
  - The policy may state that a search of the immediate work area will be:
    - Conducted by employees who work in those specified work areas and in conjunction with the security force.
    - Initiated immediately after a threat is received — regardless of the circumstances of the call.
  - In other situations, immediate evacuation and a full search by trained search teams should be conducted.
    - At most critical infrastructures, a mandatory work area search will be the best choice as an immediate first step.
    - Do not base the decision to search or evacuate solely on the appearance of the threat call's credibility.
    - Many authentic callers do not provide definitive indications that a threat is credible.
- Explain that organizations should establish guidelines for principal decisions about search and evacuation for all threats including natural disasters in the policy during the initial planning process to ensure that all response activities occur according to protocol, rather than to subjective interpretation of the situation.

| **Slide 79 Discussion Questions** |
|---|
| ▪ What is the value of assessing potential threat credibility?<br>▪ Should the building be evacuated or reoccupied before the time stated in the threat call?<br>▪ What else should you plan for in addition to bomb threats? |
| *Graphic Description: No Graphic* |

- Ask participants: **What is the value of assessing potential threat credibility?**
- Acknowledge responses. *If not provided by participants, add the following*:
  - *Strong indications of the threat's authenticity are often useful when deciding what to do once a search or evacuation is complete.*
  - *For example, what if a search is conducted and nothing is found?*

- Ask participants: **Should the building be evacuated or reoccupied before the time stated in the threat call?**
- Acknowledge responses. *If not provided by participants, add the following*:
  - *If the threat appears credible, a decision to evacuate or postpone reoccupation until after the stated time may be justified.*
- Ask participants: **What else should you plan for in addition to bomb threats?**
- Acknowledge responses. *If not provided by participants, add the following*:
  - *Planning should occur to prevent and mitigate all threats and hazards that could reasonably be expected to affect a facility' functioning; these are a few examples that require planning:*
    - *Natural disasters*
    - *Fires (accidental or man-made) — note: announcements of fires or bomb threats at public events may generate stampedes, which should be addressed in planning*
    - *Power failures*
    - *Large scale picketing-public unrest*
    - *Bio-chemical contamination*
    - *Computer server failures*
    - *Natural disasters*

**Slide 80 Step 4: Determine an Incident Command Post (1 of 2) (Workbook 11.4)**

- Bomb threat management plan should include an incident command post — the location from which the incident commander manages search and response activities
- Location depends upon the type of search and response plan

*Graphic Description: No Graphic*

- Refer participants to **Workbook 11.4: Threat Management Checklists,** *Table 2: Incident Command Post Checklist***.**
- Explain that Step 4 requires that an incident command post be included in the bomb threat management plan.
- Define **incident command post:** the location from which the incident commander manages search and response activities.
- Explain that once the bomb threat management plan is initiated, the incident commander should move control operations to the designated incident command post.
- Tell participants that the location of this command post depends upon the type of search and response plan.

**Slide 81 Step 4: Determine an Incident Command Post (2 of 2) (Workbook 11.4)**

- If an evacuation is required, relocate the incident command post to an alternate position outside of the building
- To facilitate the mobility requirements of the incident command post, create a portable incident command post kit

*Graphic Description: No Graphic*

- Explain that if an evacuation is required, the incident command post should be relocated to an alternate position outside of the building.
- Explain that preparing a portable incident command post kit to facilitate mobility is important because critical incident circumstances can often change quickly and mobility may be vital to save lives.
- Explain that Table 2 in the addendum includes information on what should be included in the incident command post kit.
  - A hard copy of the bomb threat management plan
  - A facility layout diagram (marked with evacuation routes and search zones)
  - A telephone contact sheet that includes staff names and emergency telephone numbers
  - Security team search information
  - Search zone checklist

**Slide 82 Step 5: Develop a Search and Evacuation Plan (Workbook 11.4)**

- Primary search procedures:
  - Security team
  - Employee work area
  - Law enforcement assisted
- Additional search guidance and search team safety points
- Explosive device search procedures
- Evacuation procedures

*Graphic Description: No Graphic*

- Explain that step 5 ensures development of a search and evacuation plan to include in the bomb threat management plan and specifies the steps for search and evacuation to take immediately after receipt of the bomb threat.
- Refer participants to **Workbook 11.4: Threat Management Checklists,** *Table 3: Search and Evacuation Plan***.**
- Tell participants that this table provides guidance they should include in their plan for searches by the security team, in the employee work area, and with the assistance of law enforcement. This table also provides helpful information on additional search guidance, explosive device search procedures, and evacuation procedures.

**Slide 83 Step 6: Establish a Response Procedure (1 of 2)**

- Evacuate all employees from the danger area
- Notify law enforcement
- Secure danger area to prevent accidental intrusion
- Brief bomb technicians about situation
- Warn local authorities about any potential hazards

*Graphic Description: No Graphic*

- Explain that step 6 of creating a bomb threat management plan is to establish a response procedure.

- Explain the elements of a response procedure:
  - Immediately evacuate all employees from the danger area
  - Notify law enforcement of the suspicious object situation
  - Secure the danger area to prevent accidental intrusion
  - Once law enforcement arrives, the incident commander should brief bomb technicians about the situation and on movement routes inside the facility
  - Warn authorities about any potential hazards regarding the release of chemicals or biological agents

**Slide 84 Step 6: Establish a Response Procedure (2 of 2)**

- Response procedures should:
  - Include actions to take after the suspicious object has been removed from the site
  - Consider any hazards resulting from disruption of safe process operations
  - Provide guidelines for warning local authorities about any potential hazards

*Graphic Description: No Graphic*

- Explain that the response procedures should:
  - Include actions to take after the suspicious object has been removed from the site, as well as any follow-up searches and reoccupation of the facility.
  - Consider any hazards resulting from disruption of safe process operations.
    - For example, in many facilities certain process operations must be shut down in a staged manner, or as another example, classified documents must be stored in a particular manner before all employees can evacuate.
    - If these cases, the response plan should identify who must stay behind while other employees evacuate.
  - Provide guidelines for warning local authorities whether a detonation could result in chemical or biohazard release.
- Explain to participants that this same protocol will also serve as a guide for responding to suspicious objects discovered during normal activities, as opposed to receiving a phone bomb threat.
- Tell participants that in the next section they will have an opportunity to consider the elements of such a policy.

**Slide 85 Threaded Exercise Part 4 — Bomb Threat Management Policy (Workbook Part 4)**

- Purpose: to create a bomb threat management policy for the National Ministries Building by answering a series of questions
  - Duration: 30 minutes (20-exercise; 10-debrief)
  - Group composition: table groups
  - Debrief: large-group discussion

*Graphic Description: No Graphic*

**Slide 86 National Ministries Building Complex Map (Workbook Part 4)**

- *No Text*

*Graphic Description: No Graphic*

- Refer participants to **Threaded Exercise Part 4 — Bomb Threat Management Policy**.
- Refer participants again to the National Ministries Building Complex Map for a visual representation of the National Ministries Building.
- Allow participants a few minutes to read the exercise details in the addendum.
- Review exercise directions:
  - Participants will work with their table groups to complete Table 8: Bomb Threat Management Plan Considerations using information about the National Ministries Building Complex.
  - Groups will read each line item in the **Questions** column and provide answers in the **Considerations** column.
  - Teams should be prepared to share their answers with the class.
  - They will have 20 minutes to complete Table 8.
- Explain that although they may not be able develop a complete bomb threat management policy for the National Ministries Building, this exercise will enable them to identify the various elements such a policy would require.
- Encourage participants to refer back to the policies and procedures discussed previously in this section.
- Refer to **Threaded Exercise Workbook Part 4—National Ministries Building Answer Key** for discussion and debrief.
- Lead a large-group discussion that includes each team sharing an answer from their worksheet.
- Ask teams what other information they would have liked to have to complete their plans.
- Provide overall feedback at when all questions have been answered.
- Ask participants whether they have any questions about bomb threat management policies and procedures or anything else covered thus far.

**Slide 87 TeachBack Moment**

- How do policies and procedures help the effectiveness of response to a critical incident?
- What elements should be included in a bomb threat management policy?

*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: **How do policies and procedures help the effectiveness of response to a critical incident?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Policies and procedures provide direction and guidance to security personnel during critical incidents by helping to create a critical incident management plan and working within an established critical incident management plan process*

- Ask participants: **What elements should be included in a bomb threat management policy?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Step 1: Designate management responsibilities*
  - *Step 2: Define procedures for handling bomb threat calls*
  - *Step 3: Determine procedures for evaluating bomb threat calls*
  - *Step 4: Identify an incident command post*
  - *Step 5: Develop a search and evacuation plan*
  - *Step 6: Establish a response procedure*

| **Topic: Module Summary** | **10 Minutes** |
|---|---|

| **Slide 88 Module Summary** |
|---|
| ▪ Policies and procedures relating to a physical protection system<br>▪ Types of policies and procedures to protect critical infrastructure<br>▪ Policies and procedures relating to critical incidents<br>▪ Bomb threat management plan |
| *Graphic Description: No Graphic* |

- Summarize the module by reviewing the following points:
  - **Policies and procedures relating to a physical protection system:**
    - Definitions
    - Purpose of and need for
    - Guidelines for writing policies
    - Characteristics
    - Updating
  - **Types of policies and procedures to protect critical infrastructure:**
    - Perimeter barriers
    - Lighting
    - Intruder detection systems
    - Closed-circuit television
    - Automated access control systems
    - Security officers and patrols
    - Electronic access controls
    - Lock and key controls
    - Entry control areas
    - Secure asset locations
    - Cybersecurity
    - Include policies and procedures in a standard operating procedures manual
    - Establish a security policy
  - **Policies and procedures relating to critical incidents**
    - Critical incident definition
    - Critical incident management plan

    - Critical incident management plan process: prevention, preparedness, response, and recovery
  - **Bomb threat management plan**
    - Step 1: Designate management responsibilities
    - Step 2: Define procedures for handling bomb threat calls
    - Step 3: Determine procedures for evaluating bomb threat calls
    - Step 4: Identify an incident command post
    - Step 5: Develop a search and evacuation plan
    - Step 6: Establish a response procedure
- Ask whether there are any questions about the contents of this module.
- Explain that *Module 12: Security Force Operations* will explain how to develop a security force response plan for the protection of critical infrastructure.