Module 11

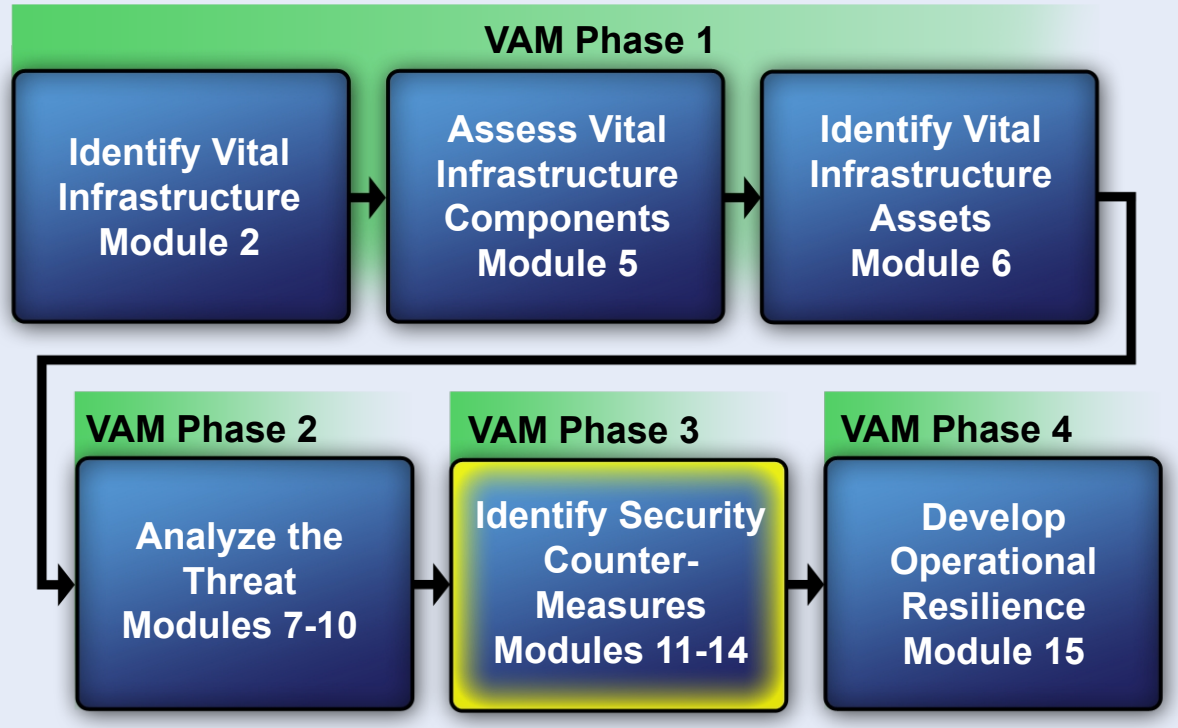
Policies and Procedures

OFFICE OF ANTITERRORISM ASSISTANCE

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

Course Map with VAM Phases



Policies and Procedures Relating to a Physical Protection System

- This section will cover:
  - Definitions
  - Purpose of and need for
  - Guidelines for writing policies
  - Characteristics
  - Updating

Definitions

- **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**

Purposes of Policies and Procedures

- Establish guidelines for security management
- Resolve security conflicts or incidents
- Ensure security of critical infrastructure
- Important for everyone:
  - Provide guidance about expectations
  - Offer a way for settling disputes

Need for Policies and Procedures (1 of 2)

Refer To:

Workbook 11.1

- If actions of employees indicate confusion about conduct
- If guidance is needed about ways to resolve conflict
- To comply with governmental policies and laws

Need for Policies and Procedures (2 of 2)

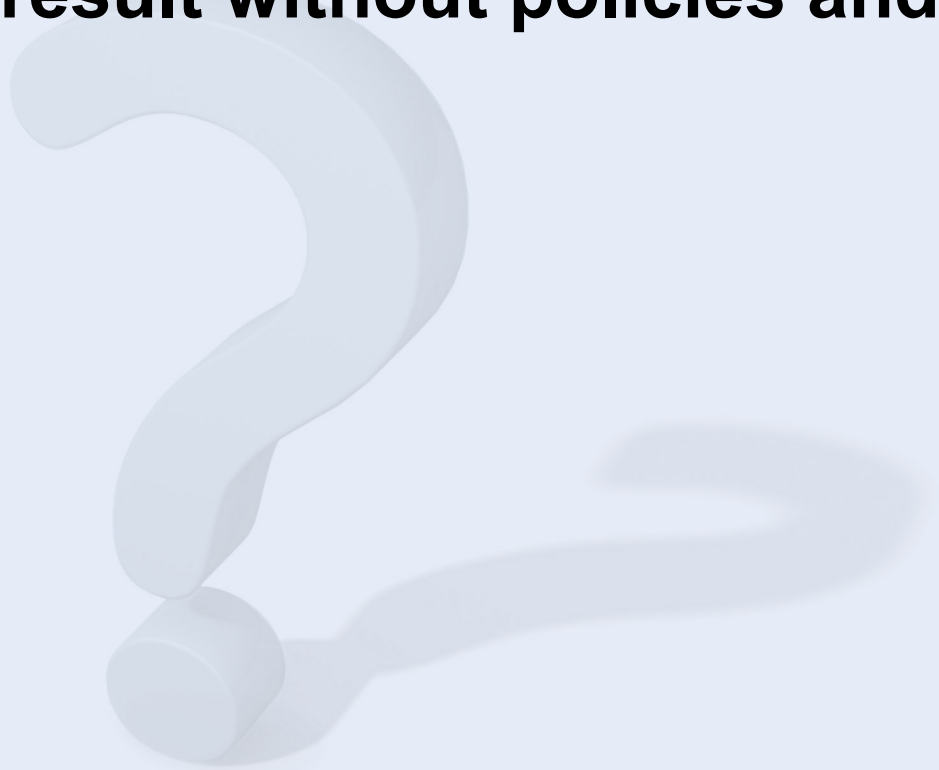
Refer To:

Workbook 11.1

- To establish consistent work standards, rules, and regulations
- To provide consistent security force response
- To ensure security technologies are functioning properly

Discussion Question

- **What consequences to critical infrastructure security might result without policies and procedures?**



Guidelines for Writing Policies

- Determine the goal to accomplish
- Tell employees why the policy is being implemented
- Provide clear and specific guidelines
- Include sufficient detail to effectively communicate the organization's position

Characteristics of Policies and Procedures

Refer To:

Workbook 11.1

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

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

Use-of-Force Procedure Example

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

Importance of Updating Policies and Procedures

- Vulnerability analysis methodology and risk assessment strategies ensure that the policies and procedures are:
  - Accurate
  - Current
  - Regularly reviewed and revised to meet changing threats

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

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

Perimeter Barrier Definition

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

Perimeter Barrier Purpose

- Delineate a boundary
- Channel visitors to legal points of entry
- Deter and delay unlawful intruders
- Provide a degree of physical, psychological, or legal deterrence

Perimeter Barrier Effectiveness (1 of 2)

- Perimeter intruder detection systems
- Closed-circuit television and security officers
- Security lighting
- Enclosed fencing

Perimeter Barrier Effectiveness (2 of 2)

- Grouped facilities
- Maintained vegetation
- Anticlimbing devices on fences
- Secure vehicle gates and fences at the same level

Perimeter Barriers Standards

Refer To:

Workbook 11.2

- Doors
- Windows
- Other areas of the facility

Lighting (1 of 2)

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

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

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

Lighting — Perimeter

- Should cast a uniform light over the perimeter
- Should create a glare that deters intruders (overhead or low-mounted lamp)
- Should not create a nuisance or hazard outside the perimeter
- Should not reveal the positions of guards, either inside or outside

Lighting — Area

- Illuminates areas inside the perimeter that intruders must cross in order to reach their objectives and:
  - Increases security officers' ability to detect intruders
  - Acts as a powerful deterrent
  - Should be even and without shadows

Intruder Detection Systems

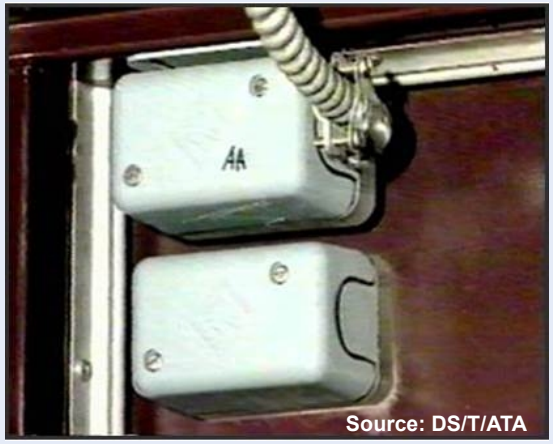
- **Designed to:**
  - Detect entry, or attempted entry, of an intruder into a protected area
  - Identify location of an intrusion
  - Signal an alarm to the security force
- **Best used to provide early detection of attack**
- **Security force must respond quickly**

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

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**



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

Closed-Circuit Television (1 of 2)

Refer To:

Workbook 11.2

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

Closed-Circuit Television (2 of 2)

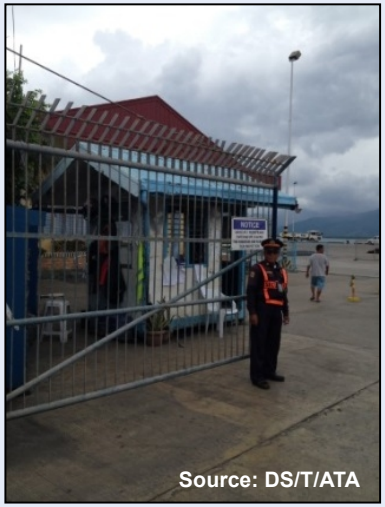
Refer To:

Workbook 11.2

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

Automated Access Control Systems

- Ensure only authorized persons gain access
- Minimum requirement: a card-access control system
- Follow standard operating procedures manual



Automated Access Control Systems — Components

- Electronic access control
- Alarm reporting
- Image capture and badge production
- Physical locks and key control
- Alarm output triggers to closed-circuit television system

Facility Access Control (1 of 2)

- Keep number of external access and exit points to a minimum
- All regular entry and exit points must be access controlled and include anti-pass backup capability

Facility Access Control (2 of 2)

- External doors with remote operation installed where entry is viewed:
  - Directly
  - By closed-circuit
- Control internal doors leading to critical areas with electronic access

Security Officers and Patrols (1 of 2)

- Where applicable, lead security officer determines security level policies and procedures based on:
  - Informed opinions on threats
  - Specific vulnerabilities
  - Identified risks

Security Officers and Patrols (2 of 2)

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

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

Lock and Key Controls

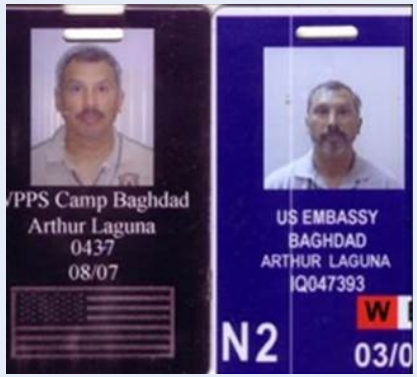
Refer To:

Workbook 11.2

- Standards
- Spare keys
- Key labeling

Entry Control Areas — Personnel

- All personnel must wear a visible identification card
- Revoke access when a staff member leaves the organization
- Verify and authorize access for any external support services personnel



Source: DS/T/ATA

Entry Control Areas — Visitors

- Ask person they are visiting to arrange access
- Obtain permission prior to the day of visit
- Be issued an identification card
- Obtain a visitor card at reception desk
- Be accompanied by an authorized person at all times

Secure Asset Locations (1 of 2)

- Locate in interior of facility
- Keep away from exterior windows
- Do not use glass doors or windows for construction
- Use metal or solid wood doors
- Control access using electronic access control with capability to maintain a record of all entrants

Secure Asset Locations (2 of 2)

- Remove exterior room door key access hardware from the master key system
- Control issuance of nonmaster keys
- Install intruder detection system with uninterrupted power source
- Do not include on floorplans and construct slab-to-slab

Source: Getty Images

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
- Keep visitors to a minimum

Security Personnel

- Control access
- Conduct building searches
- Perform patrol duties
- Use the radio to communicate
- Respond to an intrusion alarm

Types of Policies in an SOP Manual

Refer To:

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

Policies and Standard Operational Procedures (1 of 2)

Refer To:

Workbook 11.3

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

Policies and Standard Operational Procedures (2 of 2)

Refer To:

Workbook 11.3

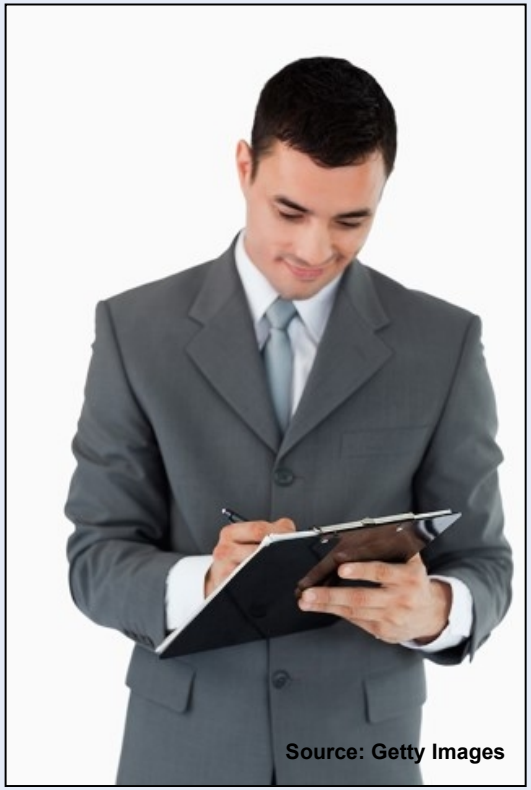
- Are reviewed annually with updates completed in a timely manner
- Provide guidance on how and when to deploy specialized units

Effective Security Policies

Refer To:

Workbook 11.3

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



Source: Getty Images

Noncompliance of Policies and Procedures

Refer To:

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

Development of a Compliance Program (1 of 2)

Refer To:

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

Development of a Compliance Program (2 of 2)

Refer To:

Workbook 11.3

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

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?

Policies and Procedures Relating to Critical Incidents

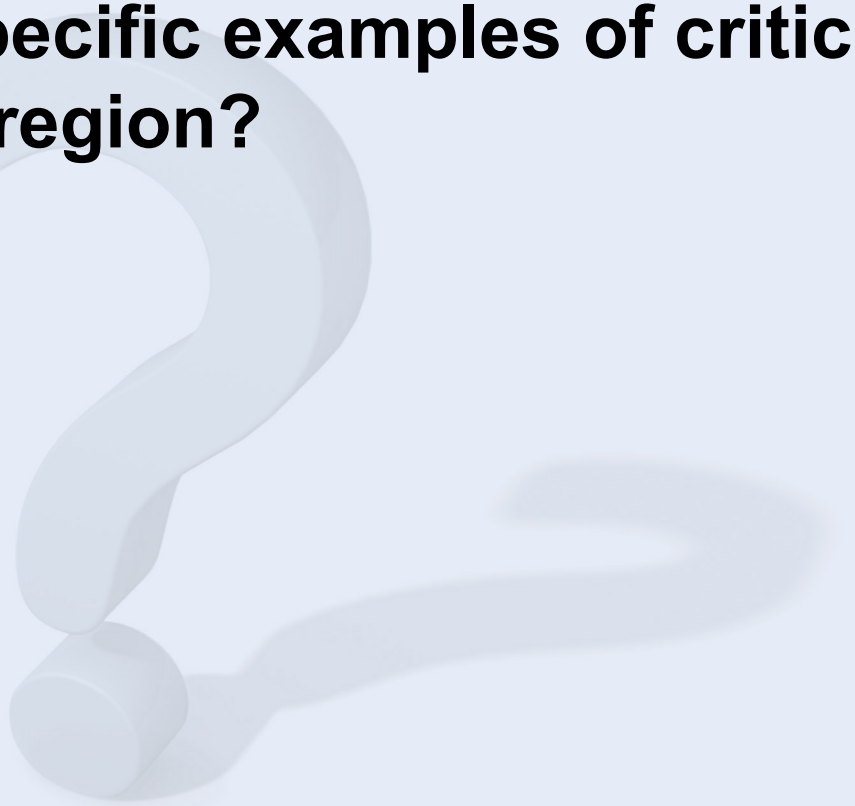
- This section will cover:
  - Critical incidents definition
  - Critical incident management plan
  - Critical incident management plan process

Critical Incident Definition

- An event of unusual or severe nature that can cause:
  - Loss of life or injury to citizens
  - Damage to property
- Critical incidents require extraordinary measures to protect lives and restore order
- Policies and procedures provide guidance for effective response

Discussion Questions

- What are some examples of critical incidents?
- What are some specific examples of critical incidents in your region?

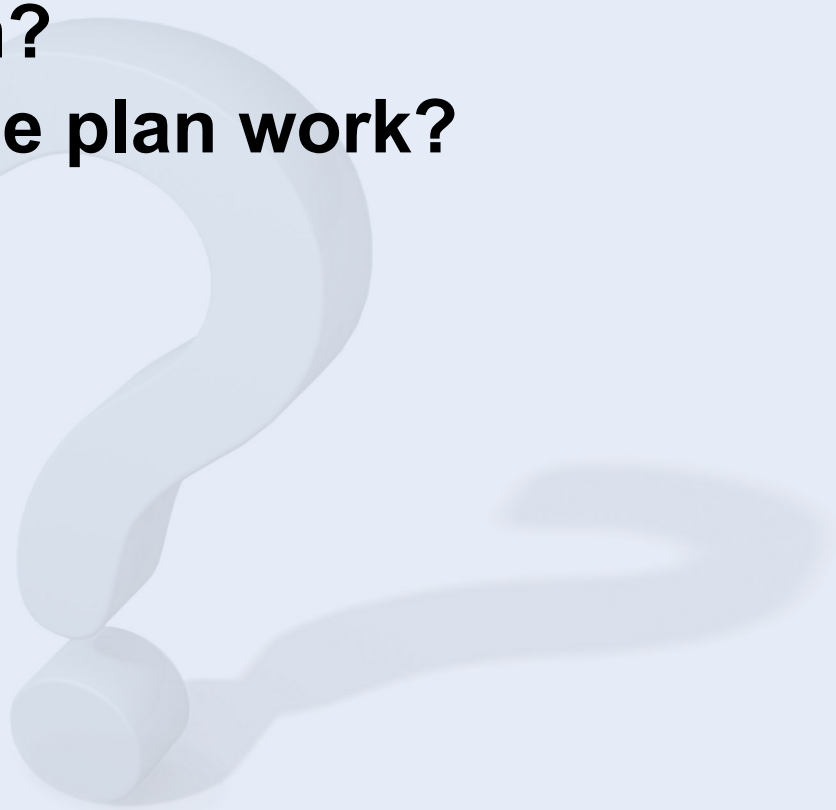


Critical Incident Management Plan

- A standardized plan that outlines processes and procedures for coordination and control of responses to a terrorism event or natural disaster

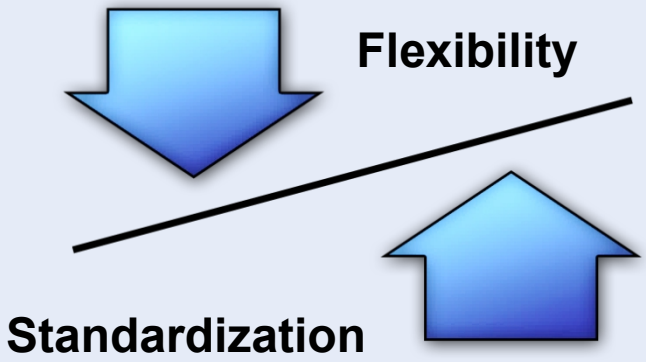
Discussion Questions

- Does your agency have a critical incident management plan?
- If so, how does the plan work?



Principles of the Critical Incident Management Process (1 of 2)

- Must be applied before, during, and after any incident
- May require multiple jurisdiction and cross-functional agency involvement
- Various responders must operate under the principles of flexibility and standardization to function as a unified team



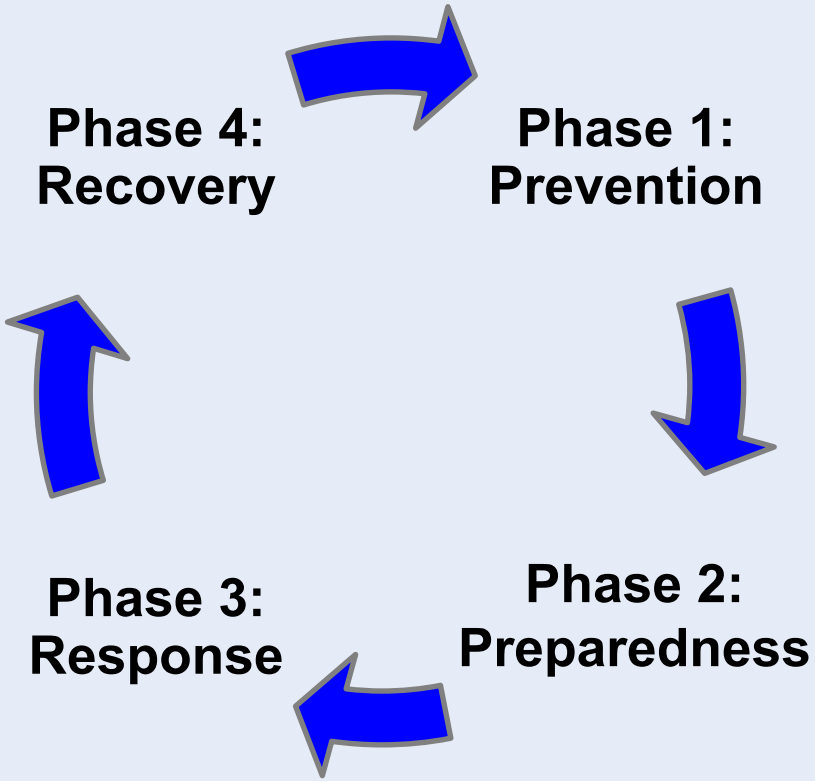
Principles of the Critical Incident Management Process (2 of 2)

- 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

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

Critical Incident Management Process Phases



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

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

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?

Step 1: Designate Management Responsibilities (1 of 4)

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

Step 1: Designate Management Responsibilities (2 of 4)

Supervisor or floor warden	Runner
Notify employees of threat	Notify supervisors and management about threat
Supervise search or evacuation activities	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**

Step 1: Designate Management Responsibilities (3 of 4)

Refer To:

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**

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


Source: Getty Images

Step 2: Define Procedures for Bomb Threat Calls (1 of 3)

Refer To:

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

Step 2: Define Procedures for Bomb Threat Calls (2 of 3)

Refer To:

Workbook 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

Step 2: Define Procedures for Bomb Threat Calls (3 of 3)

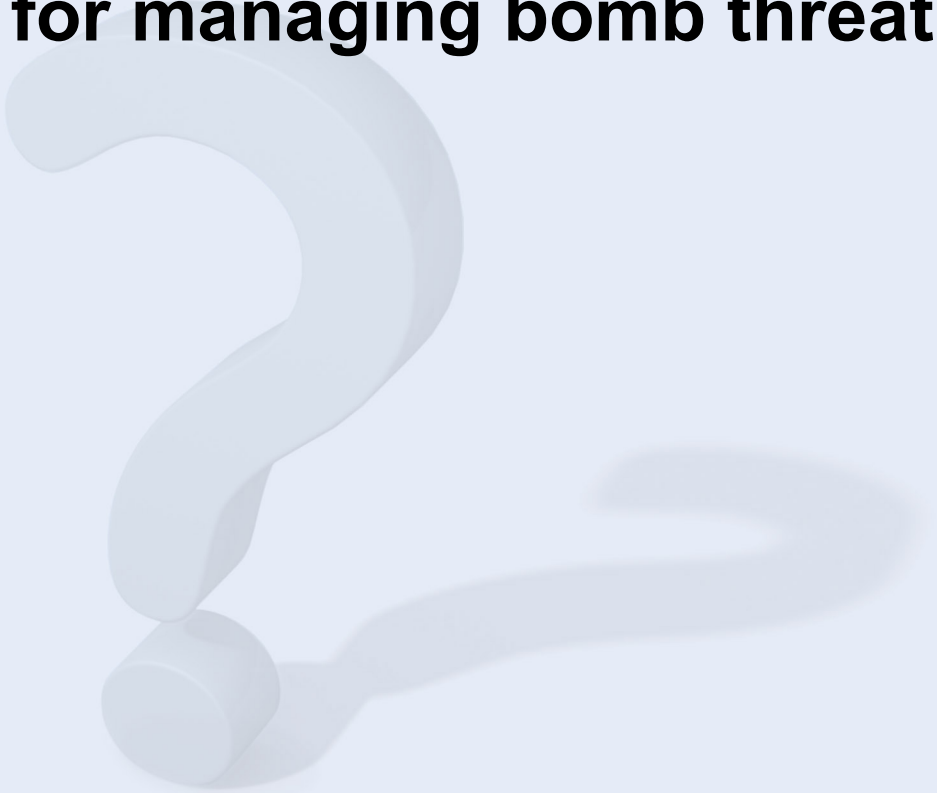
Refer To:

Workbook 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

Discussion Question

- **What existing procedures do you have in place in your agency for managing bomb threat calls?**



Step 3: Determine Procedures for Evaluating Bomb Threat Calls

- Once the threat call is received and security is notified, the incident commander should:
  - Debrief the person who received the call
  - Let the recipient of the call describe the conversation in his or her own words
  - Review the completed bomb threat checklist

How to Determine the Authenticity of a Bomb Threat

- Authentic bombers tend to:
  - Repeat the threat message in a specific manner
  - Provide detailed descriptions about the location of the device
- The more information provided, the more likely threat is real

Bomb Threat Decision Options (1 of 2)

- Evacuate
- Search
- Ignore the threat
- Do not base decisions solely on threat call's credibility

Bomb Threat Decision Options (2 of 2)

- The option chosen should be made in accordance with the bomb threat management plan
- Guidelines for decisions about search and evacuation should be established by policy

Discussion Questions

- What is the value of assessing potential threat credibility?
- Should the building be evacuated or reoccupied before the time stated in the threat call?
- What else should you plan for in addition to bomb threats?

Step 4: Determine an Incident Command Post (1 of 2)

Refer To:

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

Step 4: Determine an Incident Command Post (2 of 2)

Refer To:

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

Step 5: Develop a Search and Evacuation Plan

Refer To:

Workbook 11.4

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

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

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

Threaded Exercise Part 4 — Bomb Threat Management Policy

Refer To:

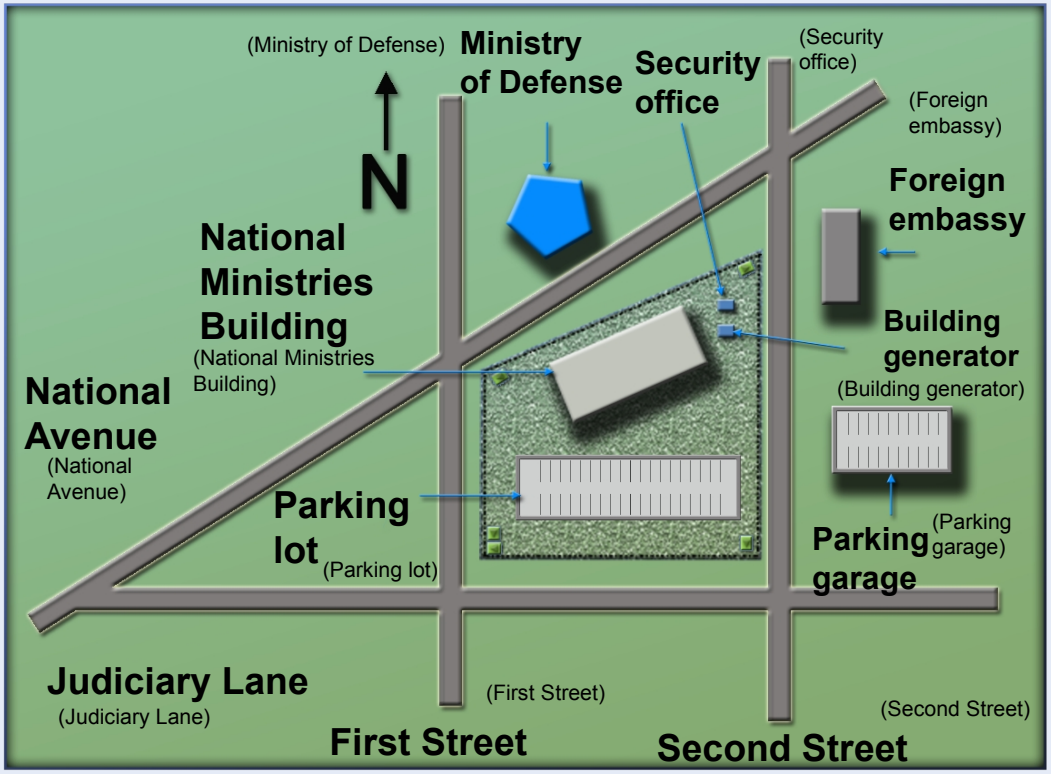
Workbook Part 4

- **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**

National Ministries Building Complex Map

Refer To:

Workbook Part 4



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?

Module Summary

- 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