Module 2

Introduction to Critical Infrastructure Security and Resilience

OFFICE OF ANTITERRORISM ASSISTANCE

Module Objective

- By the end of this module, you will be able to describe the importance of implementing a well-designed physical protection system for the security of critical infrastructure

Critical Infrastructure

- Systems and assets, whether physical or virtual, so vital to the nation that the incapacity or destruction of such systems and assets would have a debilitating impact on:
  - Security
  - National economic security
  - National public health or safety
  - Any combination of those matters

Security

- **The implementation of a set of procedures and processes that when taken as a whole have the effect of altering the ratio of undesirable events to total event based on:**
  - **Identified risks**
  - **Threats**
  - **Vulnerabilities**
  - **Probability of an undesirable occurrence**

Need for Security

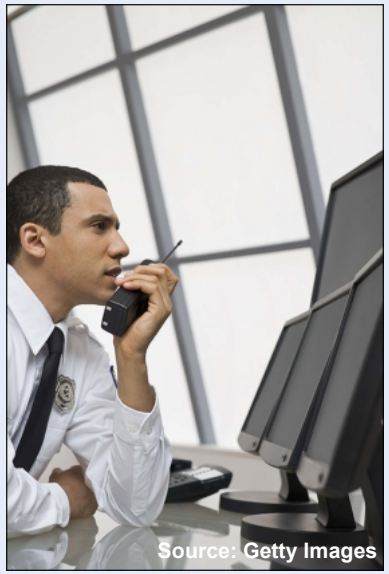
- Protect lives and property
- Sustain critical assets
- Maintain political and economic stability

Building Community Partnerships

- **Protecting and ensuring the resilience of critical infrastructure requires partnerships with multiple entities:**
  - **Government**
  - **Private sector**
  - **Academic and professional**
  - **Certain not-for-profit and private volunteer organizations**

Surveillance Awareness Overview

- A defensive security operation
- Observe, detect, and report hostile surveillance
- Crucial to protection of critical infrastructures
- Used in cyber security operations


Source: Getty Images

Vulnerability

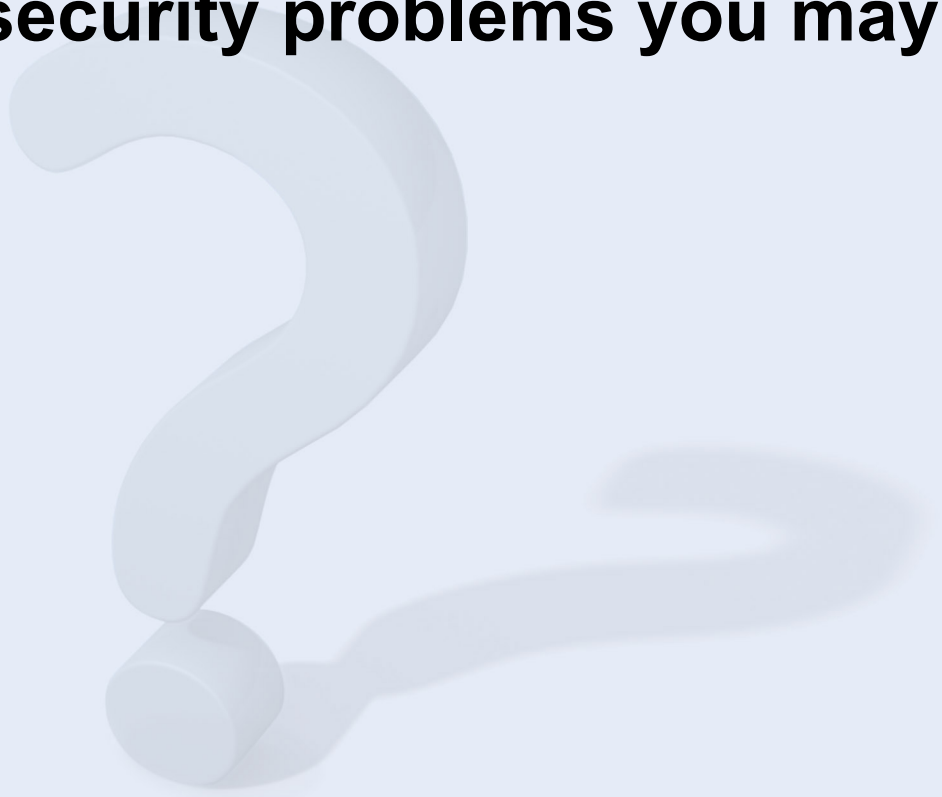
- A physical feature or operational attribute that renders an entity open to exploitation or susceptible to given threat

Vulnerability Analysis

- A product or process of identifying physical features or operational attributes that renders an entity, asset, system, network, or geographic area susceptible or exposed to threats

Discussion Question

- **What are some examples of critical infrastructure security problems you may need to address?**



Vulnerability Analysis Purpose

- Evaluate the effectiveness of implemented security countermeasures
- Preserve limited resources
- Provide security managers with accurate information in support of security decision making

TeachBack Moment

- **What is the purpose of conducting a critical infrastructure vulnerability analysis?**

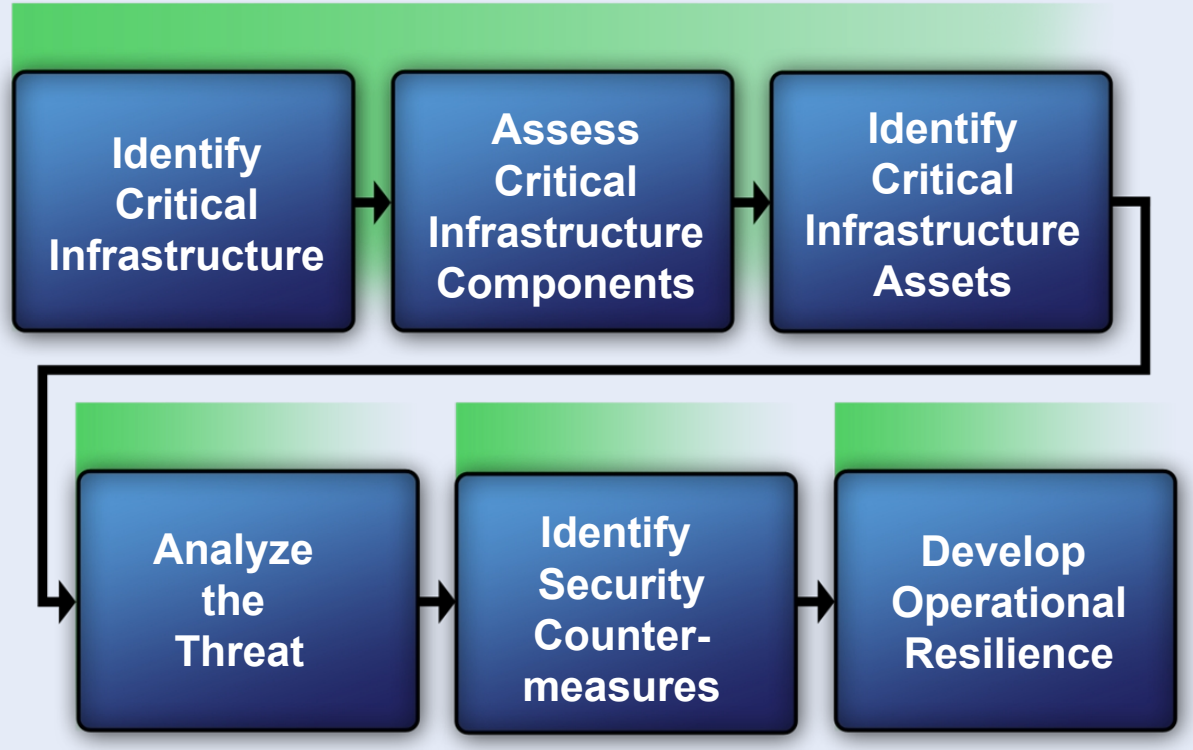
Physical Protection System Definition

- An integration of people, policies and procedures, and equipment for the protection of assets or facilities against all threats

Physical Protection System Diagram

Refer To:

Workbook 2.1



Physical Protection System Components

Refer To:

Workbook 2.1

- Design and implementation of an effective physical protection system begins with vulnerability analysis

Step 1: Identify Critical Infrastructure

Refer To:

Workbook 2.1

- Identify critical infrastructure to assess any associated security countermeasures

Critical Infrastructure Categories

Refer To:

Workbook 2.1

- What are some categories of critical infrastructure?

Step 2: Assess Critical Infrastructure Components

Refer To:

Workbook 2.1

- Environmental conditions
- Physical conditions
- Facility operations
- Facility policies and procedures
- Regulatory requirements
- Safety considerations

Purpose of Critical Infrastructure Component Assessment

- Prioritize efforts
- Use limited resources more efficiently
- Implement security countermeasures on the most important facilities

Step 3: Identify Critical Infrastructure Assets

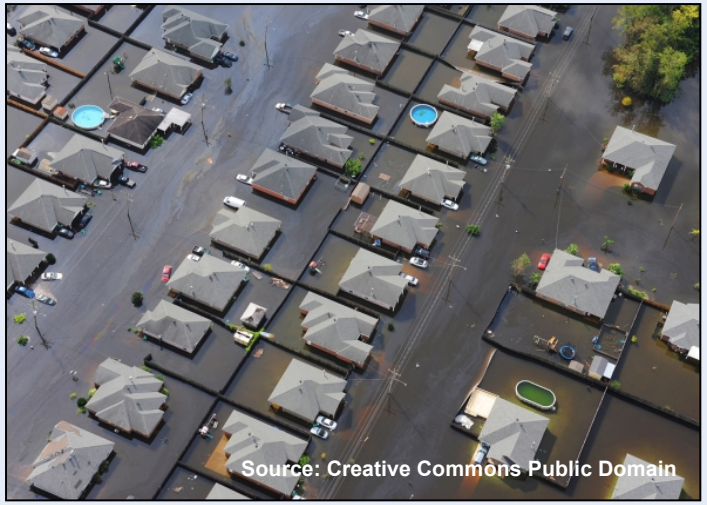
Refer To:

Workbook 2.1

- Critical assets typically are in one of four categories:
  - People
  - Information
  - Processes
  - Equipment (technology)

Prioritize Critical Infrastructure Assets

- Identify threats
- Specify undesirable consequences of loss
- Determine the probability of occurrence



Identify Threats

- Nonavailability
- Loss or theft
- Compromise
- Destruction
- Sabotage
- Assault
- Impaired operations
- Cyberattack

Undesirable Consequences of Loss

- For every asset specify all undesirable consequences of loss
- Assign values to each of the consequences specified:
  - Low
  - Medium
  - High

Probability of Occurrence

- Evaluate the probability of attack by analyzing:
  - Intelligence information
  - The effectiveness of existing security countermeasures
- Assign value of low, medium, or high to the probability

Critical Infrastructure Assets Activity

Refer To:

Handout 2.1

- **Purpose: to identify critical assets for a standard government facility that houses the Head of State or other dignitaries**
  - **Duration: 20 minutes (15-activity; 5-debrief)**
  - **Group composition: table groups**
  - **Debrief: large-group discussion**

Step 4: Analyze the Threat

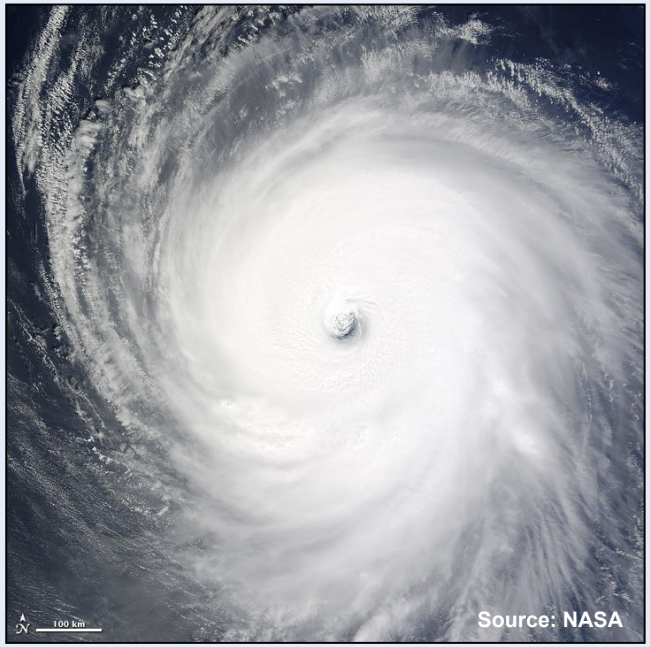
Refer To:

Workbook 2.1

- Examine the characteristics of the threat
- Formalize the information in the threat analysis statement to:
  - Summarize gathered information
  - Identify facility threats
  - Evaluate an infrastructure's physical protection system

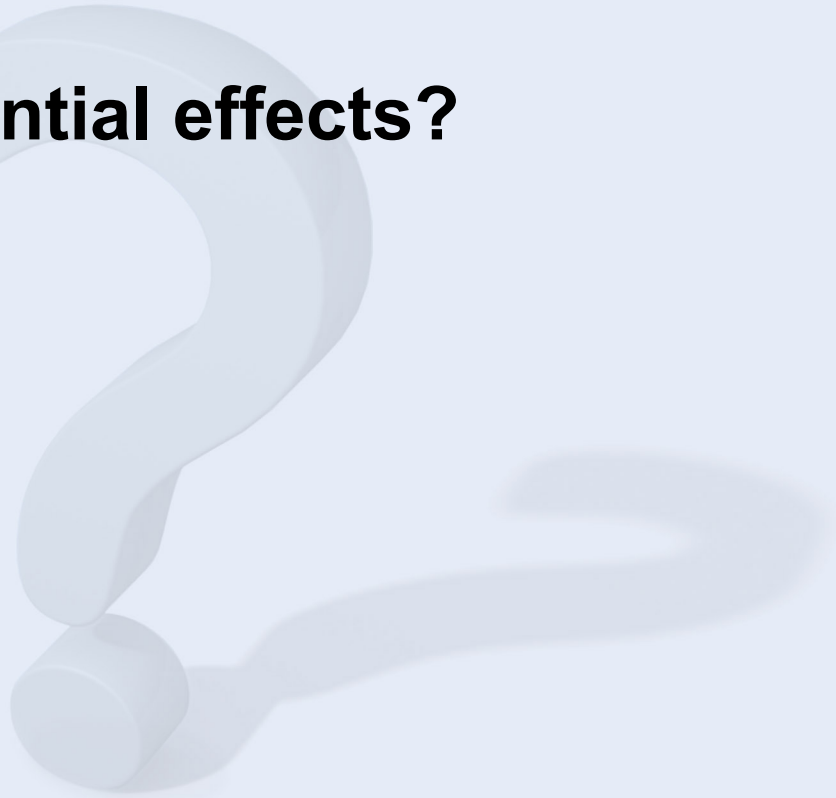
Natural Disaster Threat Characteristics to Consider

- **Before drafting the threat analysis statement, consider the following:**
  - **Type of disaster**
  - **Potential effects**
  - **Areas affected**



Discussion Questions

- What are some natural disaster threats in your area?
- What are the potential effects?



Terrorist Threat Characteristics to Consider

- **Before drafting the threat analysis statement, consider the terrorists':**
  - **Motivations**
  - **Types of threats**
  - **Equipment and weapons**
  - **Tactics**


Source: Getty Images

Discussion Question

- **Which types of terrorist threats are most likely in your region?**

Equipment and Weapons

- Knowing the range of possible weapons allows for implementation of appropriate security measures
- Terrorists typically use improvised explosive devices

Terrorist Tactics

- Force
- Stealth
- Deceit

Step 5: Security Inspection and Validation

Refer To:

Workbook 2.1

- Identify and evaluate security countermeasures:
  - Effectiveness
  - Recommendations for improvement
- Provide evaluation criteria:
  - Validate each security countermeasure
  - Determine overall effectiveness of existing physical protection system

Effective Security Countermeasures

- Should be designed to protect against the types and level of threats identified during the threat analysis

Evaluate Security Countermeasures

- To determine effectiveness, assess the following elements:
  - Policies and procedures
    - Security force
    - Technology

Policies and Procedures

- **Should focus on:**
  - **Security force**
  - **Technology**

Policies and Procedures for Security Countermeasures (1 of 2)

- **Should include:**
  - Perimeter barriers
  - Lighting
  - Intruder detection systems
  - Closed-circuit television
  - Automated access control system

Policies and Procedures for Security Countermeasures (2 of 2)

- Security officers and patrols (security force)
- Lock and key controls
- Entry control areas
- Secure asset locations
- Bomb threat management
- Information technology

Security Force Purpose

- **Effectively interrupt actions and neutralize terrorists or threats before they achieve their goal**

Security Force Elements

- **Elements that contribute to the effectiveness of a security force include:**
  - **Selection of security force members**
  - **Initial and continuous training**
  - **Deployment of adequate equipment**
  - **Appropriate supervision from command and control**

Security Force Effectiveness

- **Depends on the:**
  - **Ability to operate within established policies and procedures**
  - **Capability of the technology to detect, assess, and provide adequate delay**

Technology Purpose

- **Security managers must consider technical and nontechnical solutions that will:**
  - **Detect terrorists or intruders (intrusion detection systems)**
  - **Delay terrorists from progressing towards the target (barriers)**

Technology Elements

- Intrusion detection systems
- Barriers

Technology Supports Physical Protection System Effectiveness

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

Step 6: Develop Operational Resilience

Refer To:

Workbook 2.1

- Refine and clarify functional relationships across agencies
- Enable effective information exchange
- Implement an integration and analysis function to inform planning

TeachBack Moment

- **What are the components of a physical protection system?**

Security System Recommendations (1 of 3)

- Developed as a result from:
  - Limited scope performance testing: conducting tests on specific elements of a physical protection system
  - Gap analysis: identifying the gap between existing and required countermeasures

Security System Recommendations (2 of 3)

- Feasibility: determining whether a solution is suitable or logical
- Resilience: the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions such as deliberate attacks, accidents, or naturally occurring threats or incidents

Security System Recommendations (3 of 3)

- **Acceptability: determining whether the recommended security countermeasure provides the required protection and falls within scope of available resources**

Physical Protection System Functions

Refer To:

Workbook 2.2

- Detection and assessment
- Delay
- Response

Physical Protection System Functions Activity

Refer To:

Workbook 2.2

- **Purpose: to indicate which function of a physical protection system a specified action describes**
  - **Duration: 10 minutes (5-activity; 5-debrief)**
  - **Group composition: table groups**
  - **Debrief: large-group discussion**

Critical Infrastructure Interdependence

- Critical infrastructure is no longer limited to public works systems
- Redefined to increase security and awareness to deter attacks

Examples, Threats, and Vulnerabilities

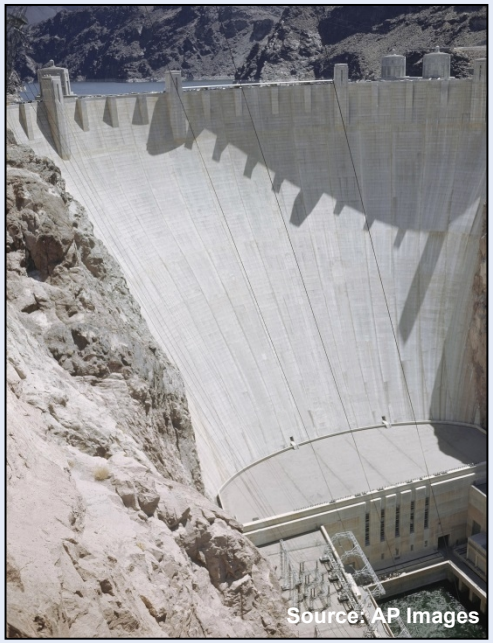
- **Necessary knowledge:**
  - **Which critical elements to protect**
  - **How to protect each critical element**
- **Must understand the threats and vulnerabilities facing the managers of critical infrastructure, in each category or sector**

Critical Infrastructure Categories (1 of 3)

Refer To:

Handout 2.2

- Chemical
- Commercial facilities
- Communications
- Critical manufacturing
- Dams



Critical Infrastructure Categories (2 of 3)

Refer To:

Handout 2.2

- Defense industrial base
- Emergency services
- Energy
- Financial services
- Food and agriculture
- Government facilities

Source: Stars and Stripes

Critical Infrastructure Categories (3 of 3)

Refer To:

Handout 2.2

- Healthcare and public health
- Information technology
- Nuclear reactors, materials, and waste
- Transportation systems
- Water and wastewater systems

Discussion Questions

- How do the earlier flip-chart responses compare with the list of categories shown?
- What are some examples of critical infrastructure that are not on this list?

Critical Infrastructure Categories Activity

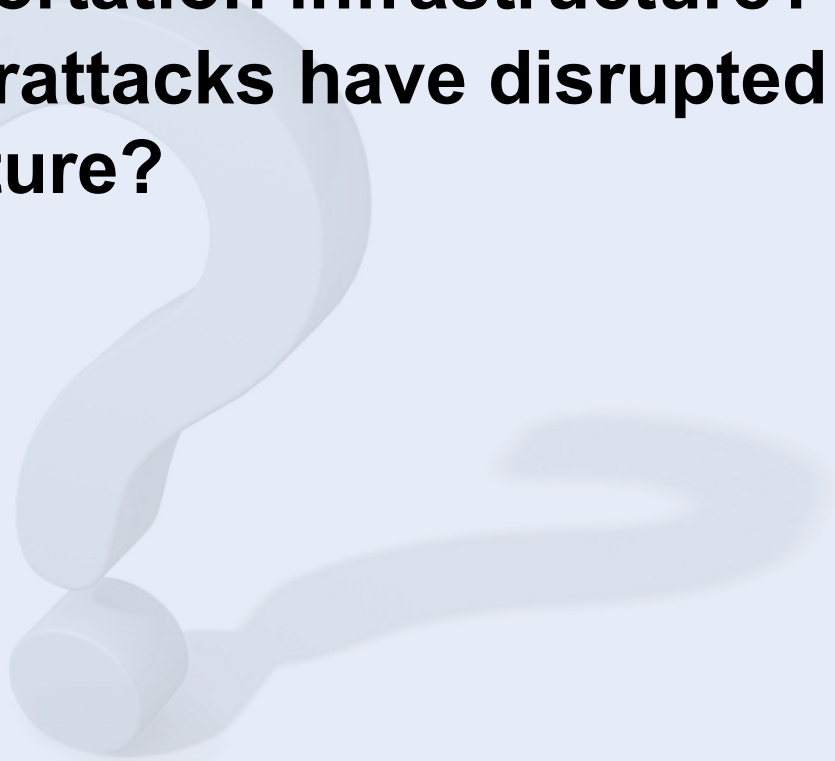
Refer To:

Handout 2.3

- **Purpose: to identify specific examples of each of the 16 critical infrastructure categories**
  - **Duration: 20 minutes (10-activity; 10-debrief)**
  - **Group composition: table groups**
  - **Debrief: large-group discussion**

Discussion Questions

- What are some examples of recent terrorist attacks on transportation infrastructure?
- What recent cyberattacks have disrupted critical infrastructure?



Vulnerability Analysis Methodology Definition

- A proven approach used to identify and mitigate security weaknesses and vulnerabilities in an infrastructure

Vulnerability Analysis Methodology Use

- **Provides the information necessary to:**
  - **Develop countermeasures for potential weaknesses**
  - **Evaluate the effectiveness of the countermeasures implemented**
  - **Make necessary changes for improvement**

Four Phases of Vulnerability Analysis Methodology (1 of 2)

Refer To:

Workbook 2.3

- **Phase 1:**
  - Identify critical infrastructure
  - Assess critical infrastructure components
  - Identify critical infrastructure assets
- **Phase 2: analyze the threat by conducting a threat analysis and providing written documentation of threat types**

Four Phases of Vulnerability Analysis Methodology (2 of 2)

Refer To:

Workbook 2.3

- **Phase 3: identify security countermeasures:**
  - Policies and procedures
  - Security force
  - Technology
- **Phase 4: develop operational resilience:**
  - Conduct a gap analysis
  - Determine actions to manage potential threats

TeachBack Moment

- **What is the importance of the information collected during the vulnerability analysis?**

Physical Protection System Report

- **Information collected in a vulnerability analysis is documented in a report that:**
  - **Identifies weaknesses**
  - **Provides a better understanding of security vulnerabilities**
  - **Provides recommendations for improvement**
  - **Assists with planning and implementation of security countermeasures**

Elements of a Physical Protection System Report (1 of 2)

- Executive summary
- Introduction
- Vulnerability analysis methodology
- Critical infrastructure identification
- Critical infrastructure component analysis

Source: Getty Images

Elements of a Physical Protection System Report (2 of 2)

- Threat definition
- Physical protection system evaluation
- Performance testing requirements
- Recommendations for improvements
- Conclusions
- References

Physical Protection System Report Discussion (1 of 3)

Refer To:

Workbook 2.4

- **Which section of the physical protection system report:**
  - **Identifies the critical infrastructure being described in the report?**
  - **Outlines the information used to locate, identify, describe, and prioritize critical infrastructure sites?**

Physical Protection System Report Discussion (2 of 3)

Refer To:

Workbook 2.4

- **Which section of the physical protection system report describes:**
  - **How physical protection system elements will be tested?**
  - **Recommendations for improving the physical protection system?**

Physical Protection System Report Discussion (3 of 3)

Refer To:

Workbook 2.4

- **Which section of the physical protection system report:**
  - **Will contain the results of the threat analysis?**
  - **Describes the processes and approaches used in the analysis?**

TeachBack Moment

- What are the four phases of the vulnerability analysis methodology?
- What information is included in each of the sections of the physical protection system report?

Module Summary (1 of 2)

- Critical infrastructure
- Security
- Vulnerability analysis
- Components, elements, and functions of a physical protection system

Module Summary (2 of 2)

- Critical infrastructure categories
- Four phases of vulnerability analysis methodology
- Elements of a physical protection system report