MODULE 2: INTRODUCTION TO CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Day: 1 Time: 4.0 Hours Level of Understanding: Comprehension

Instructional Strategies:
- Lecture
- Large-Group Discussion
- Small-Group Activity
- TeachBack Moment

Module Equipment/Facilities:
- Standard Classroom Setup
- Facilitator workbook
  - Workbook 2.2: Physical Protection System Report Discussion Answer Key
  - Handout 2.3: Critical Infrastructure Categories Activity Answer Key

Participant Materials/Handouts:
- Workbook 2.1: Physical Protection System Course Map Diagram
- Handout 2.1: Critical Infrastructure Assets Activity
- Workbook 2.2: Physical Protection System Functions & Activity
- Handout 2.2: Critical Infrastructure Categories
- Handout 2.3: Critical Infrastructure Categories Activity
- Workbook 2.3: Vulnerability Analysis Methodology Diagram
- Workbook 2.4: Physical Protection System Report Discussion

Terminal Learning 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.

Introduction

In this module, you will have an opportunity to explore ways in which you, as a security professional, can help to protect your nation's most critical facilities from potential threats. While the risk environment is ever changing and uncertain, you will need to prepare for potential threats presented from terrorist organizations, natural disasters, cyber criminals, workplace violence, and even technical malfunctions. These critical facilities are often referred to as critical infrastructure because natural disasters or successful attacks against them can undermine the stability of a nation. For this reason, you should not only

understand the types of potential threats that exist but also the ways in which a critical infrastructure's security vulnerabilities (weaknesses) can be adversely affected.

This module identifies the elements required of a well-designed security system for a critical infrastructure. You will consider all the different categories of critical infrastructure in your country and specific threats and vulnerabilities possibly associated with each. You will also learn the system's approach to vulnerability analysis using the vulnerability analysis methodology. The techniques of this methodology are designed to detect vulnerabilities and determine the level of effectiveness for a security system to protect specific targets from specific terrorist operations and other threats. Finally, you will report the information you collect during the vulnerability analysis by following the example of a logical, sequential format that this course will provide.

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
Critical Infrastructure Security	▪ Describe the need for critical infrastructure security.	10 minutes
Vulnerability Analysis	▪ Explain the purpose of conducting a critical infrastructure vulnerability analysis.	15 minutes
Physical Protection System Components	▪ Describe the components of a physical protection system.	90 minutes
Physical Protection System Functions	▪ Describe the functions of a physical protection system.	20 minutes
Critical Infrastructure Categories	▪ Describe the critical infrastructure categories.	50 minutes
Vulnerability Analysis Methodology	▪ Explain the four phases of the vulnerability analysis methodology. ▪ Explain the elements of a critical infrastructure security physical protection system report.	40 minutes
Module Summary	▪ Not Applicable	10 minutes

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

Key Terms

Key Term	Description
Asset	Person, structure, facility, information, material, or process that has value
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, or any combination of those matters
Critical infrastructure categories	The sixteen sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the nation that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health, or safety, or any combination thereof
Critical infrastructure components	The physical conditions, facility operations, policies and procedures, regulatory requirements, and the safety and legal considerations of the identified asset
Cybersecurity	Preventing damage to, unauthorized use of, or exploitation of electronic information and communication systems and databases and the information contained therein to ensure confidentiality, integrity, and availability; and restoring electronic information and communications systems in the event of a terrorist attack or natural disaster
Feasibility	Implementing security measures that are logical based on the situation and considering time, financial resources, personnel, and resources that it will take to implement
Gap analysis	The process of identifying the difference (the gap) between existing security measures and the necessary future security measure(s)
Hostile surveillance	The discreet monitoring of a person, facility, or area with the intent of gathering information to formulate a plan that will enhance the likelihood of a successful terrorist operation or attack
Improvised explosive devices	Any device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract

Key Term	Description
Limited scope performance testing	A physical protection system is likely to have many components that would require large-scale performance testing, which may be unrealistic. Instead, a limited scope performance testing can be conducted on only specific elements of a physical protection system
Physical protection system	An integration of people, policies and procedures, and equipment for the protection of assets or facilities against all threats
Policies and procedures	Basic written guidelines to ensure standard operational physical protection system effectiveness
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	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, and probability of an undesirable occurrence
Security countermeasures	An action, measure, or device intended to reduce an identified risk
Surveillance detection	A defensive security operation used to determine whether a person or persons are conducting hostile surveillance; conducted temporarily or (for some critical infrastructures) permanently by an individual or full-time by a trained team to observe, recognize, and confirm suspicious activities
Security force	A personnel-based security countermeasure
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
Vulnerability analysis methodology	A systematic approach that security experts use to detect vulnerabilities and determine the level of effectiveness of a physical protection system

Abbreviations/Acronyms

Abbreviation/Acronym	Description
PPS	Physical protection system
VAM	Vulnerability analysis methodology

Topic: Module Introduction	**10 Minutes**

Slide 1 Introduction to Critical Infrastructure Security and Resilience
▪ 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:** for activities, break class into four table groups of six participants. The same table groups will work together throughout the module.

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 importance of implementing a well-designed physical protection system for the security of critical infrastructure
Graphic Description: No Graphic

- Briefly discuss the terminal learning objective.
- Highlight the key topics to be presented:
  - Critical Infrastructure Security
  - Vulnerability Analysis
  - Physical Protection System Components
  - Critical Infrastructure Categories
- Tell the participants that the information in this module can be used to describe the importance of implementing a well-designed physical protection system for the security of critical infrastructure.

Topic: Critical Infrastructure Security — 10 Minutes

Enabling Learning Objective:
- Describe the need for critical infrastructure security.

Slide 3 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

Graphic Description: No Graphic

- Define **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, or any combination of those matters.[1]
- Provide examples of critical infrastructure:
  - Electricity
  - Water
  - Telecommunications
- Explain that what one nation might consider critical infrastructure, another nation may not. However, some categories of critical infrastructure are universal.
- Tell participants we will discuss universal categories later in the module.

Slide 4 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

Graphic Description: No Graphic

[1] USA Patriot Act of 2001, U.S.C. § 5195c(e) Section 1016(3) Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (2001)

- Define **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, and probability of an undesirable occurrence[2]
- Explain that security implies stability and a predictable environment in which people's lives are free from disruption or harm.
- Explain that the goal of security managers and stakeholders is to protect a country's critical infrastructure.

Slide 5 Need for Security
▪ Protect lives and property ▪ Sustain critical assets ▪ Maintain political and economic stability
Graphic Description: A row of security officers standing behind shields with a girl beside them

- Tell participants that designing a facility without security in mind can lead to expensive lawsuits, injuries, loss or destruction of property, and lives.
  - For example, a dam constructed without a security plan would be a target for terrorists.
    - If terrorists attack, the terrorists may damage or destroy the dam.
    - Lives could be lost, flooding could occur, and electricity generation would be hindered.
- Explain that when properly managed, effective security and terrorism-prevention operations can lead to an increase in profits and efficiency.
- Explain that security for critical infrastructure is necessary because:
  - Terrorism threatens lives and the sustainability of critical services to the infrastructure.
  - The costs associated with the loss of a critical infrastructure could be devastating to the economy.

[2] Broder, J.F. Risk Analysis and the Security Survey. 2d Ed. (Newton, MA: Butterworth-Heinemann. 2000). p. 25.

Slide 6 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
Graphic Description: No Graphic

- Tell participants that critical infrastructure security and resilience are important to the whole community.
- Define **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.[3]
- Explain that protecting and ensuring the resilience of critical infrastructure requires building collaborative partnerships with other groups in the community including:
  - Federal, state, tribal, territorial, regional, and local government entities
  - Private-sector owners and operators and representative organizations
  - Academic and professional entities
  - Certain not-for-profit and private volunteer organizations
- Tell participants that *Module 4: Building Community Partnerships* provides more detail on this topic.

Slide 7 Surveillance Awareness Overview
▪ A defensive security operation ▪ Observe, detect, and report hostile surveillance ▪ Crucial to protection of critical infrastructures ▪ Used in cybersecurity operations
Graphic Description: A man looking at a group of monitors while speaking into a handheld radio

- Explain that keeping a critical infrastructure secured requires awareness of suspicious activity and potential threat.
- Define **surveillance detection**: a defensive security operation used to determine whether a person or persons are conducting hostile surveillance; conducted

[3] USA Patriot Act of 2001, U.S.C. § 5195c(e) Section 1016(3) Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (2001)

temporarily or (for some critical infrastructures) permanently by an individual or full-time by a trained team to observe, recognize, and confirm suspicious activities.
- Define **hostile surveillance**: the discreet monitoring of a person, facility, or area with the intent of gathering information to formulate a plan that will enhance the likelihood of a successful terrorist operation or attack.
- Explain that employees, security personnel, and visitors to critical infrastructures can help by:
  - Understanding surveillance — identifying potential targets and areas where a hostile might gather information
  - Detecting surveillance — looking for unusual behaviors or activities
  - Reporting surveillance — reporting observations using predetermined procedures
- Define **cybersecurity**: preventing damage to, unauthorized use of, or exploitation of electronic information and communication systems and databases and the information contained therein to ensure confidentiality, integrity, and availability; and restoring electronic information and communications systems in the event of a terrorist attack or natural disaster
- Explain that critical infrastructures include electronic information and communication systems and surveillance detection is part of identifying those threats.
- Tell participants that *Module 7: Cybersecurity* and *Module 8: Surveillance Awareness: What You Can Do* provide more information.
- Tell participants the next topic discusses identifying critical infrastructure vulnerabilities.

Topic: Vulnerability Analysis	**15 Minutes**

Enabling Learning Objective:
- Explain the purpose of conducting a critical infrastructure vulnerability analysis.

Slide 8 Vulnerability
▪ A physical feature or operational attribute that renders an entity open to exploitation or susceptible to given threat
Graphic Description: No Graphic

- Define **vulnerability**: a physical feature or operational attribute that renders an entity open to exploitation or susceptible to given threat.
- Explain that an exploited or compromised vulnerability in a system or system component would cause an undesired result or event leading to loss or damage.

Slide 9 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
Graphic Description: No Graphic

- Define **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.
- Explain that the task of protection has become increasingly complex because:
  - Political, social, economic, and technological changes happen rapidly
  - Resources for security are more constrained
- Tell participants that a systematic approach is required for acquiring and analyzing the information necessary to support decision makers.

Slide 10 Discussion Question
▪ What are some examples of critical infrastructure security problems you may need to address?
Graphic Description: No Graphic

- Ask participants: **What are some examples of critical infrastructure security problems you may need to address?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Poor lighting at night time*
  - *Lack of security force training*
  - *Aging equipment*
  - *Lack of formal vulnerability analysis of the facility*

Slide 11 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
Graphic Description: No Graphic

- Define **security countermeasures**: an action, measure, or device intended to reduce an identified risk.
- Explain that vulnerability analysis is used to:
  - Ensure a well-designed security system by evaluating the effectiveness of proposed and implemented security countermeasures
  - Preserve limited resources by providing information that helps properly allocate resources
  - Provide security managers with accurate information used to support all decisions made regarding security

Slide 12 TeachBack Moment 
▪ What is the purpose of conducting a critical infrastructure vulnerability analysis?
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 is the purpose of conducting a critical infrastructure vulnerability analysis?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Ensure a well-designed security system by evaluating the effectiveness of proposed and implemented security countermeasures*
  - *Preserve limited resources by providing information that helps properly allocate resources*
  - *Provide security managers with accurate information used to support all decisions made regarding security*
- Ask participants whether they have any questions about anything covered thus far.
- Tell participants that the next topic discusses the components on a physical protection system.

Topic: Physical Protection System Components — 90 Minutes

Enabling Learning Objective:
- Describe the components of a physical protection system.

Slide 13 Physical Protection System Definition

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

Graphic Description: No Graphic

- Define **physical protection system**: an integration of people, procedures, and equipment for the protection of assets or facilities against all threats.
- Tell participants that this definition is applicable to all threats, which includes natural hazards such as natural disasters, terrorist attack, theft, espionage, or sabotage.
- Explain that the ultimate objective of the physical protection system is to prevent terrorists or criminals from accomplishing their desired goals.

Slide 14 Physical Protection System Diagram (Workbook 2.1)

- *No Text*

Graphic Description: Top portion of the physical protection system course map diagram showing the first six steps in the process

- Refer participants to **Workbook 2.1: Physical Protection System Course Map Diagram**.
- Tell participants that the diagram on the slide, which is the top portion of the course map, provides a visual illustration of the steps in the vulnerability analysis process.

- Explain that participants will use this diagram throughout the course to enable participants to learn the process to conduct a vulnerability analysis of a physical protection system.

Slide 15 Physical Protection System Components (Workbook 2.1)

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

Graphic Description: No Graphic

- Refer participants to **Workbook 2.1: Physical Protection System Course Map Diagram**.
- Tell participants the addendum explains how the course correlates directly to the steps of the vulnerability analysis.
- Ask a participant to read each step in the addendum.
- Explain that the design and implementation of an effective physical protection system begins with a detailed evaluation of vulnerabilities based on the specific threats for each critical infrastructure facility and the resources available.
- Explain that this module will provide an overview of the steps and that the details, methods, and strategies of each step will be discussed in further detail in subsequent modules.
- Tell participants to take notes on each step as it is discussed in the module.

Slide 16 Step 1: Identify Critical Infrastructure (Workbook 2.1)

- Identify critical infrastructure to assess any associated security countermeasures

Graphic Description: No Graphic

- Refer participants to **Workbook 2.1: Physical Protection System Course Map Diagram** to indicate step one in the process diagram.
- Tell participants that the first step in vulnerability analysis of a physical protection system is identify critical infrastructure.
- Explain the purpose of identifying critical infrastructure in a vulnerability analysis is to assess any associated security countermeasures.

Slide 17 Critical Infrastructure Categories (Workbook 2.1)

- What are some categories of critical infrastructure?

Graphic Description: No Graphic

- Remind participants of the definition of critical infrastructure.
- Tell participants that critical infrastructure can be classified in categories.
- Ask participants: **What are some categories of critical infrastructure?**
- Acknowledge responses. *Responses will vary.*

- Write the responses on a flip chart and save the pages for further discussion and comparison to the critical infrastructure categories list provided later in this module.
- Tell participants that the critical infrastructure categories will be discussed in detail later in the module.

Slide 18 Step 2: Assess Critical Infrastructure Components (Workbook 2.1)

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

Graphic Description: No Graphic

- Tell participants that the next step in vulnerability analysis is to assess critical infrastructure components.
- Refer participants to **Workbook 2.1: Physical Protection System Course Map Diagram** to indicate step two in the process diagram.
- Explain that for each facility, the critical infrastructure components to assess include:
  - Environmental conditions
  - Physical conditions
  - Facility operations
  - Facility policies and procedures
  - Regulatory requirements
  - Safety considerations

Slide 19 Purpose of Critical Infrastructure Component Assessment

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

Graphic Description: No Graphic

- Explain that the purpose of assessing critical infrastructure components is to provide security managers with valuable information which assists with:
  - Prioritizing efforts
  - Using limited resources more efficiently
  - Implementing security countermeasures on the most important facilities
- Explain that the component assessment is the basis for evaluating the effectiveness of the physical protection system.

Slide 20 Step 3: Identify Critical Infrastructure Assets (Workbook 2.1)

- Critical assets typically are in one of four categories:

- People
- Information
- Processes
- Equipment (technology)

Graphic Description: No Graphic

- Tell participants the next step in vulnerability analysis is to identify critical infrastructure assets.
- Refer participants to **Workbook 2.1: Physical Protection System Course Map Diagram** to indicate step three in the process diagram.
- Explain that critical assets typically are in four categories:
  - People
  - Information
  - Processes
  - Equipment (technology)

Slide 21 Prioritize Critical Infrastructure Assets

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

Graphic Description: Arial view of a flooded community

- Explain that the identified critical infrastructure assets also need to be prioritized to receive the correct protection. Prioritizing assets involves:
  - Identifying threats against a critical asset
  - Specifying undesirable consequences of loss associated with each critical asset
  - Determining probability of occurrence of an undesirable event associated with each critical asset

Slide 22 Identify Threats

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

Graphic Description: No Graphic

- Explain that probable threats against a critical infrastructure asset could include:
  - Nonavailability — the asset is present but cannot be accessed due to power failure, computer virus, or other reason

- Loss or theft — the asset is no longer in the possession of rightful owners
- Compromise — an unauthorized person knows specifics about the asset
- Destruction — the asset has been destroyed by natural or manmade threat
- Sabotage — the deliberate destruction of an asset to hinder or stop actions performed
- Assault — usually related to a military or paramilitary assault against an asset
- Assassination or kidnapping — involves killing or otherwise removing a human asset
- Impaired operations — the asset is unable to operate at full capacity as a result of a natural or manmade force
- Cyberattack — the asset's computer equipment or information is compromised by an unauthorized intrusion into the system

Slide 23 Undesirable Consequences of Loss

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

Graphic Description: No Graphic

- Explain that undesirable consequences of critical asset loss are the negative results of any threat or attack against a critical asset.
- Explain that after identifying the threats:
  - Specify the potential undesirable consequences of loss for each critical asset.
  - Assign each consequence of loss a value of either:
    - Low
    - Medium
    - High
- Tell participants to complete these tasks in order to ensure the accurate prioritization of assets associated with a facility.

Slide 24 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

Graphic Description: No Graphic

- Explain the process of determining the probability of occurrence of an undesirable event.
  - First evaluate the likelihood of an attack against each critical asset by analyzing the following:

    - Intelligence information about any previous attacks or threats against a facility's critical assets or any attacks or threats against a similar facility in the past
    - The effectiveness of existing security countermeasures to prevent similar attacks or threats
- Explain that after evaluating the probability of occurrence, assign assets protection values:
    - Assign the highest level of protection to those assets at the greatest risk of loss, theft, compromise, or unauthorized use. These high-value assets will most seriously affect the security, health, or safety of your nation's employees, public, environment, or programs.
    - Assign the protection of other assets based upon their value relative to available resources.
- Tell participants that *Module 6: Critical Infrastructure Assets* describes this process in detail and provides tools for analyzing assets.

Slide 25 Critical Infrastructure Assets Activity (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

Graphic Description: No Graphic

- Refer participants to **Handout 2.1: Critical Infrastructure Assets Activity**.
- Divide participants into their table groups.
- Tell participants that the purpose of this activity is to identify critical assets for a standard government facility that houses the Head of State or other dignitaries.
- Tell participants to:
    - List examples in column two of all possible critical assets for each category shown
    - Discuss with table group possible threats against the critical assets listed in each category
    - Document responses in column three
- Explain that although it may not be possible to identify a threat for every asset, participants should identify as many as they can.
- Allow 15 minutes to complete the activity.
- Ask each group to select a representative to present its information.
- Allow 5 minutes for debrief and encourage the other class participants to discuss and provide feedback.
- Tell participants that as other groups provide additional suggestions they should record these responses in their table.
- Ask participants whether they have any questions about identifying critical infrastructure assets or anything else covered thus far.

Slide 26 Step 4: Analyze the Threat (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

Graphic Description: No Graphic

- Tell participants the fourth step in vulnerability analysis is to analyze the threat.
- Refer participants to **Workbook 2.1: Physical Protection System Course Map Diagram** to indicate step four in the process diagram.
- Explain that during this step includes:
  - Gathering and examining information on the characteristics of the threat
  - Creating a formal document known as the threat analysis statement
- Explain that the threat analysis statement:
  - Summarizes the characteristics of the threat
  - Is prepared with a focus on identifying facility specific threats
  - Is used to evaluate an infrastructure's physical protection system
- Tell participants that the next slides will provide an overview of what to address in a threat analysis statement for a natural disaster and a terrorist threat.

Slide 27 Natural Disaster Threat Characteristics to Consider

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

Graphic Description: Typhoon satellite image

- Tell participants that in the case of a natural disaster the following information will help to develop a focused threat analysis statement and effective security recommendations:
  - Type of natural disaster most likely in the area
  - Potential effects of the disaster (evacuations, flooding, infrastructure damage)
  - Areas affected — geographic and infrastructure (such as power and water)
  - Resources available — emergency response groups, shelters, vital community partnership personnel

Slide 28 Discussion Questions

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

Graphic Description: No Graphic

- Ask participants: **What are some potential natural disaster threats in your area?**
- Acknowledge responses. *Responses will vary.*
- Ask participants: **What are the potential effects?**
- Acknowledge responses. *Responses will vary.*

Slide 29 Terrorist Threat Characteristics to Consider
▪ Before drafting the threat analysis statement, consider the terrorists': • Motivations • Types of threats • Equipment and weapons • Tactics
Graphic Description: Man wearing a mask using a laptop with data flowing out of it

- Tell participants that in the case of a terrorist threat the following information will help to develop a focused threat analysis statement and effective security recommendations:
  - Terrorists' motives
  - Types of threats
  - Equipment and weapons used
  - Operational tactics

Slide 30 Discussion Question
▪ Which types of terrorist threats are most likely in your region?
Graphic Description: No Graphic

- Ask participants: **Which types of terrorist threats are most likely in your region?**
- Acknowledge responses. *Responses will vary.*

Slide 31 Equipment and Weapons
▪ Knowing the range of possible weapons allows for implementation of appropriate security measures ▪ Terrorists typically use **improvised explosive devices**
Graphic Description: A bomb made of dynamite taped together with a digital detonation device attached

- Tell participants that knowing the range of possible weapons allows for implementation of appropriate security measures for critical infrastructure.
- Tell participants that terrorists typically use improvised explosive devices
- Define **improvised explosive devices**: Any device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract.
- Tell participants that *Module 9: Explosives and Critical Infrastructure* will explain more about the following:

- Design, construction, function, initiation, and delivery of improvised explosive devices
- Different types of weapons terrorists use to carry out attacks against critical infrastructure

Slide 32 Terrorist Tactics
▪ Force ▪ Stealth ▪ Deceit
Graphic Description: A woman reflected in a window who appears to be hiding

- Tell participants that a terrorist can use the following three tactics against a critical infrastructure:
  - Force — an overt attempt to overcome a physical protection security by violence, for example, blowing up a door to enter.
  - Stealth — the act of completing an adversarial task without being noticed, or going undetected, for example, the terrorist's use of pre-attack surveillance to determine areas of a fence line not visible to cameras where they could enter unobserved.
  - Deceit — the overt act of trying to deceive someone to gain access, for example using a fake picture badge to gain access to a facility by showing it to the security officer.
- Explain that development of an effective physical protection system takes all of these potential tactics into consideration.
- Tell participants that *Module 10: Analyzing the Threat*, will explain more about analyzing potential threats including the three types of terrorist tactics.

Slide 33 Step 5: Security Inspection and Validation (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
Graphic Description: No Graphic

- Tell participants that the fifth step in the vulnerability analysis is security inspection and validation that involves identifying and evaluating security countermeasures.
- Refer participants to **Workbook 2.1: Physical Protection System Course Map Diagram** to indicate step five in the process diagram.
- Explain that this step:
  - Includes evaluating existing security countermeasure for:
    - Effectiveness
    - Making recommendations for improvement

- Provides evaluation criteria to:
  - Validate each security countermeasure
  - Determine overall effectiveness of an existing physical protection system

Slide 34 Effective Security Countermeasures
▪ Should be designed to protect against the types and level of threats identified during the threat analysis
Graphic Description: A security camera

- Explain that security countermeasures should be at a level appropriate for each threat identified during the threat analysis step.

Slide 35 Evaluate Security Countermeasures
▪ To determine effectiveness, assess the following elements: • Policies and procedures • Security force • Technology
Graphic Description: A criminal with data bytes

- Explain that physical protection systems are effective when security countermeasures contain the following elements:
  - Policies and procedures
  - Security force
  - Technology
- Define **policies and procedures:** basic written guidelines to ensure standard operational physical protection system effectiveness.
- Define **security force:** a personnel-based security countermeasure.
- Tell participants that each element will be covered briefly on the next slides.

Slide 36 Policies and Procedures
▪ Should focus on: • Security force • Technology
Graphic Description: A security guard looking at the screen on an x-ray machine

- Tell participants that organizations use policy and procedure documents to record rules and regulations regarding deployment of the other two countermeasures:
  - Security force
  - Technology

Slide 37 Policies and Procedures for Security Countermeasures (1 of 2)

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

Graphic Description: No Graphic

Slide 38 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

Graphic Description: No Graphic

- Explain that policies and procedures should be included when designing security countermeasures for a critical infrastructure. Consider policies and procedures that pertain to the following:
  - Perimeter barriers
  - Lighting
  - Intruder detection systems
  - Closed-circuit television
  - Automated access control system
  - Security officers and patrols (security force)
  - Lock and key controls
  - Entry control areas
  - Secure asset locations
  - Bomb threat management
  - Information technology
- Tell participants that in addition to the numerous policies and procedures already discussed, addressing bomb threat management should be a priority:
  - Use of explosives are prevalent in terrorist attacks
  - A bomb threat received (whether verbal, written, or through other means of communication) can be significantly disruptive

Slide 39 Security Force Purpose

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

Graphic Description: Security force members with helmets on and guns drawn

- Remind participants that security force is the second element of effective security countermeasures.
- Explain that the primary purpose of the security force is to effectively interrupt terrorist action and neutralize terrorists before the terrorists' achieve their goal. This includes cyberattacks. Policies and procedures should include information on what to do to interrupt and minimize that threat. *Module 7: Cybersecurity* will provide further information on that threat.

Slide 40 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
Graphic Description: No Graphic

- Explain the primary elements that contribute to the effectiveness of a security force:
  - Selection of security force members
  - Initial and continuous training
  - Deployment of adequate equipment
  - Appropriate supervision

Slide 41 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
Graphic Description: No Graphic

- Explain that the effectiveness of a security force depends on the:
  - Ability to operate within established policies and procedures
  - Capability of the technology to detect, assess, and provide adequate delay
- Tell participants that *Module 12: Security Force Operations* will provide further detail on security force operations.
- Tell participants that *Module 14: Security Inspection and Validation*, provides an opportunity to evaluate a security force and develop a security force response plan for a given critical infrastructure.
- Ask participants whether they have any questions about anything covered thus far before transitioning to a discussion on evaluating technology as a security countermeasure.

Slide 42 Technology Purpose
▪ Security managers must consider technical and nontechnical solutions that will: • Detect terrorists or intruders • Delay terrorists from progressing towards the target
Graphic Description: Two men reviewing surveillance monitors with one on the phone appearing to alert security

- Explain that security managers must consider detection solutions that will effectively detect a terrorist or other intruder.
- Explain that security managers must also consider technical and nontechnical solutions that can delay the terrorist from progressing towards the target.

Slide 43 Technology Elements
▪ Intrusion detection systems ▪ Barriers
Graphic Description: A building with barriers at the entrance

- Tell participants that the elements of technology that help to fulfill the purpose of detect and delay include the following:
  - Intrusion detection systems
  - Barriers
- Explain that a complete intrusion detection system includes these components:
  - Intrusion sensing technology
  - Alarm communication and display
  - Alarm assessment
  - Entry and control
- Explain that delay solutions include:
  - Passive barriers remain in place all the time and include:
    - Perimeter barriers (fences, gates, vehicle barriers, and natural barriers)
    - Structural barriers (walls, doors, windows, utility ports, roofs, and floors)
  - Dispensable barriers deploy only when and where there is an attack and include:
    - Elements such as smoke or fog, polyurethane foam, sticky thermoplastic foam
    - Various entanglement devices (wire coils and nets)
  - Personnel or assigned members of the security force can be considered an element of delay if personnel are in fixed and well-protected positions.

Slide 44 Technology Supports Physical Protection System Effectiveness
▪ Protection-in-depth ▪ Minimum consequences of component failure ▪ Balanced protection
Graphic Description: A building with barriers at the entrance

- Explain that a well-engineered physical protection system that includes technology exhibits the following characteristics:
  - Protection-in-depth:
    - A physical protection system implements security countermeasures that require the terrorist to avoid or defeat a number of protective devices in sequence.
    - For example, a terrorist may need to defeat one sensor and penetrate two separate barriers before gaining entry to critical asset areas, such as a secure vault room where classified information is stored.
  - Minimum consequences of component failure:
    - Involves having a system in place that can rapidly and accurately determine the cause of component failure
    - Means also having pre-established contingency (backup) plans to ensure the system can continue to operate while the cause of failure is being assessed
  - Balanced protection:
    - No matter how a terrorist attempts to accomplish the attack goal, the terrorist will encounter effective elements of the physical protection system.
    - For example, consider the barrier surface that surrounds a room. This surface may consist of: walls, floors, and ceilings of several types; doors of several types; equipment hatches on floors and ceilings; heating, ventilation, and air conditioning openings with various types of grilles.
    - Under completely balanced protection, the time it would take to penetrate any of these barriers would be equal the time it would take security personnel to detect the penetration.
- Tell participants that *Module 13: Security Technology* will provide:
  - Detailed information about the intrusion detection system components (both technical and nontechnical solutions)
  - An opportunity to develop a technology plan for securing a given critical infrastructure providing both high and low technology solutions
- Ask participants whether they have any questions about identifying security countermeasures or anything else covered thus far.

Slide 45 Step 6: Develop Operational Resilience (Workbook 2.1)

1. Refine and clarify functional relationships across agencies
2. Enable effective information exchange
3. Implement an integration and analysis function to inform planning

Graphic Description: No Graphic

- Refer participants to **Workbook 2.1: Physical Protection System Diagram Course Map** to indicate step six in the process diagram.
- Explain that the following three items are critical objectives that **must be met in order** to strengthen critical infrastructure security and resilience:
  1. Refine and clarify functional relationships across the agencies to advance the unity of effort to strengthen critical infrastructure security and resilience.
  2. Enable effective information exchange by identifying baseline data and systems requirements.

3. Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure.

- Tell participants that *Module 15: Operational Resilience* will provide detailed information on the requirements.

Slide 46 TeachBack Moment

- What are the components of a physical protection system?

Graphic Description: No Graphic

- Conduct a TeachBack moment to assess how well the participants understand the content presented in this section of the module.
- Ask participants: **What are the components of a physical protection system?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Identify critical infrastructure*
  - *Assess critical infrastructure components*
  - *Identify critical infrastructure assets*
    - *Critical assets typically fall into one of four categories: people, information processes Equipment*
  - *Analyze the threat*
    - *Consider to draft a threat analysis statement: motivations, types of threats, equipment and weapons, tactics*
  - *Identify security countermeasures*
    - *Effective security countermeasures are at an appropriate level for the types of threats identified during the threat analysis*
    - *Assess the following elements: policies and procedures that focus on protection, security force personnel trained to detect and respond to threats, and technology designed to detect, delay, and respond to threats or attacks*
  - *Develop operational resilience*
- Ask participants whether they have any questions about physical protection system components or anything else covered thus far before transitioning to security system recommendations.

Slide 47 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

Graphic Description: No Graphic

Slide 48 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
Graphic Description: No Graphic

Slide 49 Security System Recommendations (3 of 3)
• Acceptability: determining whether the recommended security countermeasure provides the required protection and falls within scope of available resources
Graphic Description: No Graphic

- Tell participants that after conducting a vulnerability analysis make security recommendations from the information gathered. This should include efforts to develop operational resilience.
- Explain that security recommendations are developed from the following:
  -
  - Limited scope performance testing — a physical protection system is likely to have many components. Conducting large-scale performance testing for these components may be unrealistic. Instead, a limited scope performance testing can be conducted on only specific elements of a physical protection system
  - Gap analysis — the process of identifying the difference (the gap) between existing security measures and the necessary future security measure(s)
  - Feasibility — critical infrastructure management can choose to implement numerous security measures as part of a physical protection system. However, not all of those measures may be suitable or logical based on the situation. A security measure may be possible, but it may not be feasible given the time, financial resources, personnel, and resources that it will take to implement.
  - Resilience — preparations for adapting, withstanding and recovering rapidly from disruptions such as deliberate attacks.
  - Acceptability — a security countermeasure that meets the security needs of the critical infrastructure within the scope of available resources. Acceptability implies that recommended security countermeasures provide the required protection, but do not include the high, unrealistic costs associated with the implementation of other measures.
- Tell participants that *Module 15: Operational Resilience* contains further information on the gap analysis and resilience.
- Tell participants that the next topic discusses physical protection system functions.

Topic: Physical Protection System Functions	**20 Minutes**

Enabling Learning Objective:
- Describe the functions of a physical protection system.

Slide 50 Physical Protection System Functions (Workbook 2.2) 
▪ Detection and assessment

- Delay
- Response

Graphic Description: No Graphic

- Refer participants to **Workbook 2.2: Physical Protection System Functions & Activity, Part 1: Functions of a Physical Protection System**.
- Use the information in the addendum to briefly discuss the diagram and the functions of a physical protection system:
  - Detection and assessment
  - Delay
  - Response

Slide 51 Physical Protection System Functions Activity (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

Graphic Description: No Graphic

- Refer participants to **Workbook 2.2: Physical Protection System Functions & Activity, Part 2: Physical Protection System Functions Activity**.
- Divide participants into their table groups.
- Tell participants that the purpose of this activity is to indicate which function of the physical protection system a specified action describes.
- Tell participants to:
  - Complete Table 1: Physical Protection System Functions Activity:
    - Indicate which function of the physical protection system the action describes.
    - Write a brief explanation of your choice of function.
  - Be prepared to share your answers with the class.
- Allow 5 minutes to complete the activity.
- Ask each group to select a representative to present its information.
- Allow 5 minutes for debrief and encourage the other class participants to discuss and provide feedback.

Topic: Critical Infrastructure Categories — 50 Minutes

Enabling Learning Objective:

- Describe the critical infrastructure categories.

Slide 52 Critical Infrastructure Interdependence

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

Graphic Description: No Graphic

- Explain that previously critical infrastructure was considered limited to a nation's public works system.
  - With the increasing threat of international terrorism, governments adapted and redefined what is considered critical infrastructure.
  - By identifying and adding other critical assets to the list of critical infrastructure, nations can increase security and awareness to help deter potential attacks.
  - For example, in the past, educational facilities were not necessarily considered critical infrastructure. This was reconsidered after acts of terrorism against educational facilities, such as the 2004 school hostage situation in Beslan, Russian Federation and the 2007 massacre at the Virginia Polytechnic Institute and State University ("Virginia Tech") in Blacksburg, Virginia, occurred.

Slide 53 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

Graphic Description: No Graphic

- Explain that as the course progresses, participants are expected to gain a basic working knowledge of:
  - The critical elements of each of the critical infrastructures
  - Ways to protect each critical element
- Explain that participants must understand the threats and vulnerabilities facing the managers of critical infrastructure in each category, or sector, specifically related to vulnerable access areas and threats to the asset.

Slide 54 Critical Infrastructure Categories (1 of 3) (Handout 2.2)

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

Graphic Description: An aerial view of a dam

Slide 55 Critical Infrastructure Categories (2 of 3) (Handout 2.2)

- Defense industrial base
- Emergency services
- Energy
- Financial services

- Food and agriculture
- Government facilities

Graphic Description: Military base and helicopter

Slide 56 Critical Infrastructure Categories (3 of 3) (Handout 2.2)

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

Graphic Description: Train tanker cars parked beside a track

- Tell participants that they can classify critical infrastructure into 16 categories.
- Refer participants to **Handout 2.2: Critical Infrastructure Categories.**
- Explain the purpose of this addendum is to define each category of critical infrastructure and present examples and planning considerations necessary when conducting a vulnerability assessment.
- Discuss the categories in the addendum including the following for each category:
  - Definition
  - Examples
  - Threats and vulnerabilities
  - Planning considerations
- Note: if participants demonstrated familiarity with the categories, you can quickly present this material without going into much detail.

Slide 57 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?

Graphic Description: No Graphic

- Remind participants of the discussion previously conducted on critical infrastructure categories. Refer to the flip chart on which you recorded participant responses to the discussion question on critical infrastructure categories.
- Ask participants: **How do the earlier flip-chart responses compare with the list of categories shown?**
- Acknowledge responses: *If not provided by participants, add the following as applicable:*
  - *Identified many of the same categories*
  - *Left a few of the categories out*
  - *Listed specific facilities in the categories*
- Ask participants: **What are some examples of critical infrastructure that are not on this list?**
- Acknowledge responses. *Responses will vary.*

Slide 58 Critical Infrastructure Categories Activity (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

Graphic Description: No Graphic

- Refer participants to **Handout 2.3: Critical Infrastructure Categories Activity.**
- Divide participants into their table groups.
- Tell participants that the purpose of this activity is to identify specific examples of each of the 16 critical infrastructure categories.
- Tell participants to:
  - Complete Table 1: Categories of Critical Infrastructure — Examples
  - Record specific examples for each category in column two
  - Be prepared to share answers with the class
- Allow 10 minutes to complete the activity.
- Ask each group to select a representative to present its information.
- Allow 10 minutes for debrief and encourage the other class participants to discuss and provide feedback.

Slide 59 Discussion Questions

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

Graphic Description: No Graphic

- Ask participants: **What are some examples of recent terrorist attacks on transportation infrastructure?**
  - Acknowledge responses. *If not provided by participants, provide examples:*
  - Note: If there are more recent examples, refer to them. It is not important to present case studies here, simply provide examples of how transportation infrastructure is a common target of terrorist attack.
    - *23 December 2015 cyberattacks on power grids in Ukraine*
    - *24 January 2011 terrorist suicide bombing attack at the Moscow Airport*
    - *29 March 2010 Moscow Metro Bombings by women suicide bombers*
    - *30 June 2007 Glasgow International Airport attack by two men using a vehicle-borne improvised explosive device*
    - *11 June 2006 bombings on Mumbai India's transit system during the evening rush hour, beginning with a railway station in a northwest suburb*
    - *7 July 2005 bombings on London's public transportation system, including their underground system (referred to as the "Tube") and a double-decker bus*
    - *11 March 2004 Madrid train bombings*
- Ask participants: **What recent cyberattacks have disrupted critical infrastructure?**

  - Acknowledge responses. *If not provided by participants, provide examples such as:*
    - *23 December 2015 cyberattacks by Russian hacking group Sandworm on power grids in Ukraine resulted in 80,000 residents losing power for six hours.*
- Ask participants for other examples of this critical infrastructure in their nation and write responses on the flip chart for reference when discussing transportation, postal, and shipping systems infrastructure. Briefly discuss threats and vulnerable access areas potentially associated with each.
- Tell participants that this sector will be discussed further in *Module 5: Critical Infrastructure Components* and *Module 6: Critical Infrastructure Assets*.

Topic: Vulnerability Analysis Methodology	**40 Minutes**

Enabling Learning Objectives:
- Explain the four phases of the vulnerability analysis methodology.
- Explain the elements of a critical infrastructure security physical protection system report.

Slide 60 Vulnerability Analysis Methodology Definition
▪ A proven approach used to identify and mitigate security weaknesses and vulnerabilities in an infrastructure
Graphic Description: Examining facility through night vision

- Define **vulnerability analysis methodology**: a proven approach used to identify and mitigate security weaknesses and vulnerabilities in an infrastructure.
- Note: remember this section is an introduction only to the vulnerability analysis methodology and it will be discussed in more detail throughout the training. Do not discuss this content in detail at this point.

Slide 61 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
Graphic Description: No Graphic

- Explain the importance of conducting a vulnerability analysis using the vulnerability analysis methodology in protecting critical infrastructure.
  - After establishing and categorizing critical infrastructure, conduct a vulnerability analysis using a systematic process, or methodology, to ensure protection of the most appropriate infrastructure against viable threats.
  - A vulnerability analysis conducted using the vulnerability analysis methodology will provide the information necessary to:
    - Develop countermeasures for potential weaknesses

- Evaluate the effectiveness of the countermeasures implemented
- Make necessary changes for improvement

Slide 62 Four Phases of Vulnerability Analysis Methodology (1 of 2) (Workbook 2.3)

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

Graphic Description: No Graphic

Slide 63 Four Phases of Vulnerability Analysis Methodology (2 of 2) (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

Graphic Description: No Graphic

- Refer participants to **Workbook 2.3: Vulnerability Analysis Methodology Diagram**.
- Explain that there are four phases in the vulnerability analysis methodology and that the four phases include the steps in the vulnerability analysis.
  - Phase 1 involves identifying critical infrastructure, evaluating components, and identifying the critical infrastructure assets that need protection.
  - Phase 2 is conducting the threat analysis to provide written documentation of the types of threats a specific critical infrastructure could encounter.
  - Phase 3 identifies the three types of security countermeasures necessary to interrupt and neutralize terrorists:
    - Policies and procedures
    - Technology
    - Security force recommendations
  - Phase 4 develop operational resilience, which includes:
    - Conducting a gap analysis in order to determine the security measure to implement
    - Conducting a limited scope performance test on specified elements of the system
    - Identifying security measures that are feasible to implement
    - Making preparations for adapting to, with standing, or recovering from an attack
    - Determining acceptable levels of protection
- Explain that the course layout correlates with the phases of vulnerability analysis methodology and topics will be discussed in detail in subsequent modules.

Slide 64 TeachBack Moment

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

Graphic Description: No Graphic

- Ask participants: **What is the importance of the information collected during the vulnerability analysis?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Helps build a better knowledge of the facility and potential threats from the terrorist to ensure security*
  - *Helps develop recommendations for improvements*

Slide 65 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

Graphic Description: No Graphic

- Explain that information collected during the vulnerability analysis becomes part of the physical protection system report.
- Tell participants this report is intended to:
  - Identify weaknesses
  - Provide a better understanding of security vulnerabilities in a given critical infrastructure
  - Provide recommendations for improvement
  - Assist with planning, developing, and implementing the most effective security countermeasures to deter or mitigate potential terrorist attacks

Slide 66 Elements of a Physical Protection System Report (1 of 2)

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

Graphic Description: Hand with pen and report binder

- Explain that the physical protection system report consists of many elements. Each element is beneficial to providing a comprehensive, effective report.
- Explain the elements of a physical protection system report:
  - The **executive summary** summarizes the vulnerability analysis methodology, providing an overview of the security status of the facility.

- The summary includes a description of the facility, vulnerabilities, threats, and recommendations for improvement.
- The **introduction** section includes the purpose of the vulnerability analysis and which areas were analyzed.
- The **vulnerability analysis methodology** section of the report outlines the processes and approaches used in the analysis.
- The **critical infrastructure identification** section includes descriptions of the critical infrastructure identified and which of those may be targets.
- The **critical infrastructure component analysis** section provides a visual picture of the facility, including photographs, diagrams, maps and protection system capabilities.

Slide 67 Elements of a Physical Protection System Report (2 of 2)

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

Graphic Description: No Graphic

- Explain the remaining sections of the physical protection system report:
  - The **threat definition** section of the physical protection system report describes the threat and any related adversary plans and strategies. This section also includes the threat analysis statement to include any additional site-specific threat information.
  - The **physical protection system evaluation** section discusses how to evaluate the physical security systems and what constitutes a level of acceptable performance.
  - The **performance testing requirements** section explains the testing criteria for protection elements and the processes used.
  - The **recommendations** for improvements section of the analysis describes further analysis needed to implement cost effective recommendations for improvements.
  - The **conclusions** section describes the facility's current protection level and any recommendations to employ to enhance security and efficiency.
  - The **references** section includes any references used during the analysis. Some common examples are guidance documents, site plans, specialized reports, and past performance results.

Slide 68 Physical Protection System Report Discussion (1 of 3) (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?

Graphic Description: No Graphic

Slide 69 Physical Protection System Report Discussion (2 of 3) (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?

Graphic Description: No Graphic

Slide 70 Physical Protection System Report Discussion (3 of 3) (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?

Graphic Description: No Graphic

- Refer participants to **Workbook 2.4: Physical Protection System Report Discussion** and allow a few minutes for the participants to read the information.
- Read the elements of a physical protection system report as shown in the addendum.
- Ask participants whether there are any questions about the report.
- Lead a 20-minute large-group discussion on the type of material that belongs in each section of the report.
- Ask participants: **Which section of the physical protection system report identifies the critical infrastructure being described in the report?**
- Acknowledge responses. *If not provided by participants, add the following: Introduction*
- Ask participants: **Which section of the physical protection system report outlines the information used to locate, identify, describe, and prioritize critical infrastructure sites?**
- Acknowledge responses. *If not provided by participants, add the following: critical infrastructure identification*
- Ask participants: **Which section of the physical protection system report describes how physical protection system elements will be tested?**
- Acknowledge responses. *If not provided by participants, add the following: performance testing requirements*
- Ask participants: **Which section of the physical protection system report describes recommendations for improving the physical protection system?**
- Acknowledge responses. *If not provided by participants, add the following: conclusions*
- Ask participants: **Which section of the physical protection system report will contain the results of the threat analysis?**
- Acknowledge responses. *If not provided by participants, add the following: threat definition*
- Ask participants: **Which section of the physical protection system report describes the processes and approaches used in the analysis?**
- Acknowledge responses. *If not provided by participants, add the following: vulnerability analysis methodology*

- Explain that participants will complete sections of the physical protection system report as part of their vulnerability analysis in several subsequent modules based on information they collect for a given critical infrastructure in a threaded scenario.
- Tell participants that they will conduct a vulnerability analysis on a selected critical infrastructure as part of the final exercise for this course.

Slide 71 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?

Graphic Description: No Graphic

- Conduct a TeachBack moment to assess how well the participants understand the content presented in this section of the module.
- Ask participants: **What are the four phases of the vulnerability analysis methodology?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Identify critical infrastructure, evaluate critical infrastructure components , identify the critical assets*
  - *Analyze the threat*
  - *Recommend security countermeasures*
  - *Operational resilience*
- Ask participants: **What information is included in each of the sections of the physical protection system report?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Introduction:*
    - *Critical infrastructure identification: outlines the information used to locate, identify, describe, and prioritize critical infrastructure sites*
    - *Performance testing requirements: describes how physical protection system elements will be tested*
  - *Conclusions:*
    - *Defines recommendations for improvement*
    - *Threat definition: contains the results of the threat analysis*
    - *Vulnerability analysis methodology: describes the processes and approaches used in the analysis*

Topic: Module Summary **15 Minutes**

Slide 72 Module Summary (1 of 2)
▪ Critical infrastructure ▪ Security ▪ Vulnerability analysis ▪ Components, elements, and functions of a physical protection system
Graphic Description: No Graphic

Slide 73 Module Summary (2 of 2) (Addendum 2.8)
▪ Critical infrastructure categories ▪ Four phases of vulnerability analysis methodology ▪ Elements of a physical protection system report
Graphic Description: No Graphic

- Summarize the module by reviewing the following points:
  - **Critical infrastructure security —** 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, or any combination of these matters.
    - Security
    - Need for security
    - Surveillance detection and awareness
  - **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.
  - **Physical protection system components**
    - Step 1: identify critical infrastructure
    - Step 2: assess critical infrastructure components
    - Step 3: identify critical infrastructure assets
    - Step 4: analyze the threat
    - Step 5: security inspection and validation
    - Step 6: develop operational resilience
  - **Critical infrastructure categories:**
    - Chemical
    - Commercial facilities
    - Communications
    - Critical manufacturing
    - Dams
    - Defense industrial base
    - Emergency services
    - Energy
    - Financial services
    - Food and agriculture
    - Government facilities

    - Healthcare and public health
    - Information technology
    - Nuclear reactors, materials, and waste
    - Transportation systems
    - Water and wastewater systems
  - **Vulnerability analysis methodology:**
    - Phase 1: identify critical infrastructure; assess critical infrastructure and components; identify critical infrastructure assets
    - Phase 2: analyze the threat by conducting a threat analysis and providing written documentation of threat types
    - 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
  - Ask whether there are any questions about the contents of this module.
- Explain that *Module 3: Community Engagement and Human Rights* will explain the importance of community engagement and human rights in deterring terrorism.

This Page Intentionally Left Blank.