MODULE 5: CRITICAL INFRASTRUCTURE COMPONENTS

Day: 2 **Time:** 4.0 Hours **Level of Understanding:** Application

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

Module Equipment/Facilities:
- Standard Classroom Setup
- Threaded Exercise Workbook introduction and Part 1—National Ministries Building Answer Key
- National Ministries Building Complex Map

Participant Materials/Handouts:
- Workbook 2.1: Physical Protection System Course Map Diagram
- Addendum 5.2: Gathering Component Data
- Threaded Exercise Workbook Introduction and Part 1 — National Ministries Building

Terminal Learning Objective

By the end of this module, you will be able to determine the components of critical infrastructure to establish the basis of a vulnerability analysis.

Introduction

Once you have identified the critical infrastructure, the next step is to assess the critical infrastructure by evaluating the components. Critical infrastructure components are the physical conditions, facility operations, policies and procedures, regulatory requirements, and the safety and legal considerations of the identified asset. This step — assess critical infrastructure components — is second on the Physical Protection System Diagram and forms the basis for the vulnerability analysis. This step is critical to your ability to evaluate the security for a particular critical infrastructure.

This module introduces the components of critical infrastructure security and explains the importance of these components when conducting the vulnerability analysis. This module will also cover the methodology for gathering necessary information for facilities so that you have the information you need to make an accurate assessment of the existing security measures. At the end of this module, you will complete the first part of the Threaded Exercise Workbook Introduction and Part 1 — National Ministries Building. The threaded exercise describes a scenario-based progressive learning activity that builds upon the learning objectives outlined in the modules in which the exercise occurs. This exercise will

prepare you for the important task of conducting a vulnerability analysis of a specific critical infrastructure.

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 Assessments	▪ Describe the components used in critical infrastructure assessments.	85 minutes
Critical Infrastructure Components	▪ Explain how critical infrastructure components are used in critical infrastructure assessments.	35 minutes
Threaded Exercise Introduction and Part 1—National Ministries Building	▪ Evaluate the critical infrastructure components for a critical asset in a given scenario.	100 minutes
Module Summary	▪ Not Applicable	15 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
Critical infrastructure assessment	A comprehensive evaluation of the critical infrastructure components of a given critical infrastructure
Data call	To request information about the site prior to actually performing the site visit
European Union	A group or confederation of European countries that adheres to a standardized system of laws
Secondary critical assets	Secure areas that are accessible only after entrance through a primary access controlled entry
Security control center	A room or building that serves as the primary command and communication hub for all security-related information and systems
Threaded exercise	A scenario-based progressive learning activity that builds upon the learning objectives outlined in the modules in which the exercise occurs

Key Term	Description
Vulnerability analysis team	The people responsible for planning, conducting, and reporting on a vulnerability analysis; team members of may include a project manager, a security system technologist(s), and subject matter experts from the site

Abbreviations/Acronyms

Abbreviation/Acronym	Description
VAM	Vulnerability analysis methodology

Topic: Module Introduction — 5 Minutes

Slide 1 Components of Critical Infrastructure

- 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:
  - This module is divided into approximately two and a half hours for lecture, discussion, and demonstration and one hour and a half for the Threaded Exercise Workbook Introduction and Part 1 — National Ministries Building.
  - You will divide participants into small groups during this module to assess critical infrastructure components given a scenario and facility layout.
  - Prior to start of this course, you should have gathered information about the host training facility, using the recommended characterization methodology presented in this course (planning, data review, site visit, and information evaluation).
  - In the event you were not able to gather information about the host training facility, be prepared (when prompted) to describe to participants how you would have applied the recommended methodology phases and what information you would have gathered, specific to the host training facility.

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 the 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 determine the components of critical infrastructure to establish the basis of a vulnerability analysis

Graphic Description: No Graphic

- Briefly discuss the terminal learning objective.
- Highlight the key topics to be presented:

- Critical Infrastructure Assessments
- Critical Infrastructure Components

- Tell the participants that the information in this module can be used to assess components of critical infrastructure. This assessment establishes the basis of a vulnerability analysis.

Slide 3 Course Map with VAM Phases (Workbook 2.1)

- *No Text*

Graphic Description: Top portion of the course map with VAM phases with the block containing Assess Critical Infrastructure Components Module 5 highlighted

- Refer participants to **Workbook 2.1: Course Map with VAM Phases.**
- Explain that after identifying the critical infrastructure, the next step of vulnerability analysis methodology (VAM) is to assess the critical infrastructure components of the asset.
- Remind participants that the vulnerability analysis methodology was discussed in *Module 2: Introduction to Critical Infrastructure Security and Resilience.*
- Tell participants that assessing critical infrastructure and its components are part of phase one of the vulnerability assessment methodology.

Topic: Critical Infrastructure Assessments **85 Minutes**

Enabling Learning Objective:

- Describe the critical infrastructure components used in critical infrastructure assessments.

Slide 4 Critical Infrastructure Components Defined

- The physical conditions, facility operations, policies, and procedures, regulatory requirements, and the safety and legal considerations of the identified asset

Graphic Description: No Graphic

- Remind participants of the definition for **critical infrastructure components** in *Module 2: Introduction to Critical Infrastructure and Resilience*: the physical conditions, facility operations, policies, and procedures, regulatory requirements, and the safety and legal considerations of the identified asset.
- Tell participants the importance of these components in developing a vulnerability analysis will be discussed later in the module.

Slide 5 Critical Infrastructure Assessment Defined
▪ A comprehensive evaluation of the components of a given critical infrastructure
Graphic Description: Man assessing facility

- Define **critical infrastructure assessment**: a comprehensive evaluation of the components of a given critical infrastructure.
- Explain that evaluation of critical infrastructure components occurs during a critical infrastructure assessment.

Slide 6 Purpose of Critical Infrastructure Assessments
▪ Provide a comprehensive evaluation of a critical infrastructure's components ▪ Assess and mitigate vulnerabilities ▪ Identify and establish security countermeasures
Graphic Description: Group of men in hard hats inspecting a structure

- Explain that the purpose of a critical infrastructure assessment is to:
  - Provide a comprehensive evaluation of the critical infrastructure components
  - Assess and mitigate potential security vulnerabilities
  - Identify and establish security countermeasures
- Remind participants that these initial assessments are the basis for the vulnerability analysis.

Slide 7 Evaluation of Critical Infrastructure Components
▪ Is part of the process of securing facilities against all threats including terrorist attack and natural disasters ▪ Requires a methodical approach ▪ Involves gathering data such as: • Physical description of the facility • Known vulnerabilities and weaknesses
Graphic Description: No Graphic

- Explain that evaluation of critical infrastructure components:
  - Is part of the process security managers and coordinators use to secure facilities against all threats including a terrorist attack and natural disasters.
  - Requires a methodical approach that:
    - Allows full access to the facility, its technical drawings, and other related resources
    - Helps to develop a clear understanding of the site
  - Involves gathering data such as:
    - A physical description of the facility
    - Any known vulnerabilities and weaknesses

Slide 8 Accurate Data
▪ Gathering accurate information is critical ▪ Accurate data allows for the development of appropriate security countermeasure recommendations
Graphic Description: Workers evaluating building plan

- Explain the importance of accurate data collection as part of these initial assessments. Accurate data allows for correct analysis of vulnerabilities. Correct analysis of specific vulnerabilities ensures that decision makers have what is needed to accomplish the goal to mitigate vulnerabilities.
- Tell participants that accurate data enables security managers and coordinators to develop appropriate countermeasure recommendations.

Slide 9 Inaccurate Data
▪ Results in: • Wasted resources • Damage or destruction of critical assets • Injury or death
Graphic Description: Money on fire

- Explain that the risks associated with inaccurate data include:
  - Wasted resources
  - Damage or destruction of critical assets
  - Injury or possibly death
- Tell participants that later in this module, an appropriate method for collecting data will be discussed.

Slide 10 Critical Infrastructure Components
▪ This section will cover: • Physical conditions • Facility operations, policies, and procedures • Regulatory requirements • Safety considerations • Legal considerations
Graphic Description: No Graphic

- Write these components on a flip chart. Use the chart for discussion and comparison later in the module.
  - Physical conditions
  - Facility operations, policies, and procedures
  - Regulatory requirements
  - Safety considerations
  - Legal considerations

- Explain that proper assessment of a critical infrastructure includes data collected on the components listed.
- Tell participants that the next slides discuss each critical infrastructure component.

Slide 11 Physical Conditions Component (1 of 2)
▪ Site boundaries ▪ Number and location of buildings ▪ Room locations within buildings ▪ Access points
Graphic Description: No Graphic

Slide 12 Physical Conditions Component (2 of 2)
▪ Existing physical protection system ▪ Building construction details ▪ Environmental aspects
Graphic Description: No Graphic

- Explain that data is collected during a critical infrastructure assessment on the following physical conditions:
  - The site boundary
  - Number and location of buildings in the complex
  - Room locations within buildings
  - Access points
  - Existing physical security protection system
  - Building construction details of the critical infrastructure
  - Environmental aspects

Slide 13 Environmental Aspects
▪ Topography ▪ Vegetation ▪ Wildlife ▪ Background noise ▪ Climate and weather conditions
Graphic Description: 3-D topographical map

- Explain that environmental aspects can affect access and are important considerations to terrorists when planning an attack and for first responders in the event of an attack.
- Tell participants that environmental aspects are also important to understanding potential vulnerabilities in the event of a natural disaster.
- Tell participants that environmental aspects include the following and provide examples:
  - **Topography** (surface features and elevation) — knowing if the facility is at a low or higher elevation, away from urban areas or easily accessible, or near any bodies of

water helps those planning an attack and those who need to mitigate the attack or provide emergency services.
- **Vegetation** —vegetation around the facility can be analyzed to determine how it might provide cover for terrorists, impede progress for first responders, or may cause destruction or limit access in a natural disaster.
- **Wildlife** — in the area could pose a danger during any catastrophic event.
- **Background noise** — for example, noise generated by airports or factories may limit the ability of security to hear intruders or hinder first responders attempting to locate victims.
- **Climate for the region and weather conditions** — typical local climate can help to identify times when certain natural disasters, such as typhoons, are more likely to occur. Terrorists will determine when weather conditions would be more favorable for them when launching an attack.

Slide 14 Knowledge of Physical Conditions
▪ Helps to identify conditions that may limit site access: • Vegetation • Isolation ▪ Used to predict terrorist routes into the facility and best routes for security force and first responders
Graphic Description: Arial view of a large public facility including buildings, recreation areas, vegetation, roads, and surrounding area

- Explain that knowledge gained about the physical conditions of a site can identify conditions that limit site access, such as vegetation and isolation.
- Explain that this knowledge can also be used to predict possible terrorist routes into the facility and best routes for security force and first responders.

Slide 15 Discussion Question
▪ Can you provide examples of physical conditions that have influenced the design of a physical protection system?
Graphic Description: No Graphic

- Ask participants: **Can you provide examples of physical conditions that have influenced the design of a physical protection system?**
- Acknowledge responses. *If necessary provide an example from your experience or use the following:*
    - *Facility managers can use vegetation around the perimeter of the critical infrastructure to block the view from outsiders.*
    - *Facility designers may use the terrain to hide the facility in a valley area away from the view of normal foot or vehicle traffic.*
    - *Facility designers may build a nuclear site on an island to limit access.*

Slide 16 Facility Operations Component
▪ Process and products — facility assets ▪ Operating conditions: • Hours of operation • Number of employees • Staff and visitors' movement • Traffic patterns and specialized equipment
Graphic Description: A power plant in operation at sunset

- Explain that when assessing facility operations, data collection focuses on:
  - Process and products are the assets of the facility, such as the equipment or machinery used to create a product. For example, a power plant uses special equipment and machinery to produce electricity.
  - Operating conditions are examined to identify:
    - How the facility is staffed while conducting open including hours of operation and numbers of employees working each shift, including weekdays, weekends, and holidays
    - Frequency of staff and visitor movement inside buildings
    - Vehicle traffic patterns
    - Other specialized equipment usage, such as heavy equipment like cranes and forklifts
- Explain that a thorough assessment of the operations will help identify potential constraints in establishing a protective strategy for critical assets.

Slide 17 Facility Polices and Procedures Component
▪ Documented policies and procedures ▪ Employee training ▪ Disciplinary action procedures for policy violations ▪ Proper supervision and management
Graphic Description: Group of people seated in a conference room with binders and books open and a trainer standing and looking over the table

- Explain that all facilities should have documented policies and procedures to ensure the facility functions properly and securely. This includes plans for:
  - Maintenance
  - Security
  - Evacuation
- Explain the following about facility policies and procedures:
  - Employees should receive training on policies and procedures affecting their job.
  - Disciplinary actions for violations of a policy should be a part of the overall policy statement so that the employees understand the consequences for violating security policies and procedures. If violations that occur are documented, the reports will help determine if any vulnerability exists in the physical protection system.

    - For example, the facility has a requirement for employees to escort visitors while on the premises.
    - Failure to escort visitors is a violation and the employee should receive a written disciplinary warning with the first violation.
    - Documenting every incident, every time, will indicate if other similar disciplinary reports exist, and identify repeat offenders.
- Tell participants that in some cases, the policies and procedures may state a certain guideline but implementation is quite different:
    - For example, a facility may have a policy requiring all packages go through an x-ray machine before delivery to the designated location.
    - What may really occur is that all packages delivered to the shipping area go through the x-ray machine, but packages delivered to the receptionist desk do not.
- Explain that while managers set the policies and procedures, supervisors are responsible for ensuring compliance.

Slide 18 Regulatory Requirements Component
▪ Collect data on regulatory requirements and standards that apply to the facility ▪ Ensure that the physical protection system design does not conflict with regulations
Graphic Description: Security guard outside facility

- Tell participants that, typically, critical infrastructures are regulated by a government regulatory authority that may include:
    - Local emergency services responders
    - National government agencies
    - Special interest groups
- Explain that in some cases the regulatory authority will mandate specific security requirements for selected facilities. For example, in the United States, the Nuclear Regulatory Commission mandates the type of security measures implemented at a nuclear power generating facility.
- Explain that data collected on regulatory requirements affects the physical protection system design.
    - The physical protection system may have to conform to regulations and cannot conflict with the regulations and standards the facility is required to meet.
    - For example, some countries have regulations that require all buildings to include emergency exits. The regulatory authority in those countries will not permit any proposed security measure that violates the regulated safety concern, such as blocking emergency exits.

Slide 19 Safety Considerations Component
▪ Before implementing security countermeasures: • Consult the safety authority at the critical infrastructure • Ensure compliance with safety regulations and policies ▪ The vulnerability analysis team may not include a safety expert
Graphic Description: Man dressed in safety gear checking pipes and valves

- Explain that before implementing security countermeasures, participants should:
  - Consult the safety authority at the critical infrastructure
  - Ensure compliance with safety regulations and policies
- Define **vulnerability analysis team:** the people responsible for planning, conducting, and reporting on a vulnerability analysis; team members may include a project manager, a security system technologist(s), and subject matter experts from the site.
- Tell participants that vulnerability analysis teams may not include a safety expert.
- Tell participants they will learn more about the composition of the vulnerability analysis team later in the module.
- Explain that unintentional safety issues can arise when aspects of the planned security measures are not considered.
  - For example, a release that opens a door electronically with the push of the button can fail.
  - In one facility using that system, water from the automatic sprinklers shorted the electronic mechanism, causing the door to remain locked.
  - The facility installed an automatic release mechanism that works even if there is no power.

Slide 20 Discussion Question
▪ What are some examples of other safety considerations for critical infrastructure in your country?
Graphic Description: No Graphic

- Ask participants: **What are some examples of other safety considerations for critical infrastructure in your country?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Evacuation routes during emergencies*
  - *Hazardous materials*
  - *Dangerous areas, such as shooting ranges*

Slide 21 Legal Considerations Component (1 of 3)
▪ Collect data on legal information to ensure the physical protection system does not create legal problems for the facility
Graphic Description: Gold balance scales

- Explain that gathering information on legal considerations is important when collecting data about a facility.
- Tell participants that legal information is used to ensure the physical protection system does not create legal problems for the facility.

Slide 22 Legal Considerations Component (2 of 3)
▪ May include:

- Use-of-force policy
- Employee rights and privacy concerns when conducting searches of employees and visitors
- Training requirements for security force

Graphic Description: No Graphic

- Explain that legal considerations may include:
  - Security force's use-of-force policy
  - Employee rights and privacy concerns when conducting searches of employees and visitors
  - Training requirements for security force personnel

Slide 23 Legal Considerations Component (3 of 3)

- Failure to comply with legal requirements could result in:
  - Financial penalties for the facility
  - Prison time for senior executives
  - Litigation (civil lawsuits)

Graphic Description: Outside a federal prison

- Explain that failure to comply with legal requirements is similar to a failure to comply with regulatory requirements; violations can result in:
  - Financial penalties for the facility
  - Prison time for senior executives
  - Litigation (civil lawsuits)
- Provide the following examples:
  - The failure to provide legislative mandated security countermeasures could have implications for legal liability.
    - For example, it may be mandated that a particular number of security force members is required to respond to a critical asset should a terrorist attack occur.
    - If that number does not respond, the facility would be in violation.
    - This is often observed in cases dealing with radioactive material (nuclear power facilities) where the country has mandated a specific number of security force members to protect against a specific threat.
  - A security force that fails to comply with their use-of-force policy in arresting a terrorist may be subject to legal consequences.
    - For example, the security force used excessive force in the arrest.
    - Failure to train the security force properly may be a legal problem for the critical infrastructure executive staff.

Slide 24 TeachBack Moment 
▪ What are some examples of the components used to assess critical infrastructure?
Graphic Description: No Graphic

- Conduct a TeachBack moment to assess how well the participants understand the content presented in this section of the module.
- Use the flip chart created previously listing the critical infrastructure components.
- Ask participants: **What are some examples of the components used to assess critical infrastructure?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Environment and physical conditions: maps, building diagrams, weather conditions, topography*
  - *Facility operations: processes, operating conditions, schedules, numbers of employees, vehicle traffic*
  - *Facility policies and procedures: visitor policies, incoming package policies, disciplinary policies*
  - *Regulatory requirements: required security countermeasures*
  - *Safety considerations: security systems causing safety issues*
  - *Legal considerations: employees' rights, privacy, security force training*
- Write the participant responses on the flip chart next to their corresponding components.

Topic: Critical Infrastructure Components **35 Minutes**

Enabling Learning Objective:
- Explain how critical infrastructure components are used in critical infrastructure assessments.

Slide 25 Critical Infrastructure Components
▪ This section will cover: • Critical infrastructure components evaluation • Methodology for gathering information on the facilities critical infrastructure components
Graphic Description: No Graphic

- Tell participants that this topic will explain the:
  - Importance of evaluating critical infrastructure components of a facility
  - Methodology for gathering the information on critical infrastructure components when assessing a facility

Slide 26 Critical Infrastructure Component Evaluation
▪ Allows security managers to: • Protect critical assets • Prioritize efforts • Use limited resources more efficiently
Graphic Description: No Graphic

- Tell participants that the critical infrastructure component evaluation must be conducted before a vulnerability analysis can be conducted.
- Explain the importance of the critical infrastructure component evaluation:
  - Evaluating critical infrastructure components of a facility:
    - Primarily ensures that a vulnerability analysis is conducted on the facility that is deemed to be the most critical
    - Provides information that allows security managers to determine the prioritized order for protection and allocation of resources
  - Not having the proper evaluation of critical infrastructure components can cause:
    - Waste of human resource hours assessing a less critical facility
    - Financial resources being spent on unnecessary security countermeasures
    - Less resources available to protect a facility from terrorist attacks, if limited resources were wasted

Slide 27 Prioritize Vulnerability Analysis Efforts
▪ Identify: • Critical assets • Common vulnerabilities and protection solutions • Interdependencies between infrastructures
Graphic Description: Building after a disaster with rubble all around

- Explain that the vulnerability analysis process uses a systematic approach to solving problems dealing with prioritization of critical infrastructure.
- Tell participants policy makers try to prioritize efforts by identifying these elements:
  - Critical assets — prioritization generally begins with assessing critical infrastructure components
  - Common vulnerabilities and protection solutions
  - Interdependencies between critical infrastructure asset
- Tell participants that prioritization is important since policy makers must balance preparations for two types of events.
  - Those with a low probability of occurring, but which, if they did occur, could be catastrophic
  - Those that are less catastrophic, but could happen more easily
- Tell participants that next slides will discuss the process for prioritizing vulnerability analysis efforts.

Slide 28 Identify Critical Assets
▪ Focus on identifying the truly critical assets ▪ Harden critical assets against attack ▪ If possible, reduce the effect of asset loss through: • Redundancy • Relocation • Redesign
Graphic Description: Building with gates protecting entrance

- Tell participants to focus on identifying truly critical assets.
  - Explain that some critical assets are:
    - Low cost
    - Easily replaceable equipment or portions of an infrastructure
    - May be less critical or somewhat redundant to other operations
  - Explain that if these assets were unusable, the loss would be an inconvenience but not devastating.
- Explain that governments may use critical infrastructure component evaluations to decide which facilities are most critical by:
  - Determining:
    - Expected impact and likelihood of catastrophic events
    - Redundancies among similar facilities
    - Vulnerabilities that affect multiple infrastructures
  - Identifying:
    - Interdependencies
    - Geographic relationships
    - Government responsibility versus private sector responsibility
- Explain that identifying the truly critical assets allows protections to be added that harden (or toughen) the critical asset against attack.
- Tell participants they will need to ensure effect of asset loss is mitigated through the following:
  - Redundancy
  - Relocation
  - Redesign
- Provide the following examples:
  - **Redundancy:**
    - One type of redundancy includes storing information technology data at another facility away from the primary structure.
    - This ensures data is backed up and secure in the event the primary facility suffers an attack or natural disaster.
  - **Relocation:** If a facility is located in a coastal area and may be subject to rising tides and sea level fluctuations due to climate change, it might be reasonable to consider relocating the facility.
  - **Redesign:**
    - A critical infrastructure facility may need to be redesigned if it is codependent on another form of critical infrastructure.

    - If a facility is required to have power to operate and that power is no longer available, it might be advisable to redesign that facility to be able to operate on or with a back-up power source.
- Explain that participants will learn more details about the importance of focusing on elements within a given critical infrastructure in *Module 6: Critical Infrastructure Assets.*

Slide 29 Identify Common Vulnerabilities and Protection Solutions
▪ Establish and implement best practices: • Methods that show consistent superior results • Benchmarks • Variable to each asset
Graphic Description: View of hurricane from above

- Provide examples of common vulnerabilities and protection solutions:
  - Multiple critical infrastructures can share information systems, such as computer networks.
  - Solutions include establishing and implementing best practices or developing more secure software.
  - Another example is remote control systems, such as alarms or automated maintenance procedures that personnel can initiate from a location other than the facility.
- Tell participants that security managers should consider these common vulnerabilities and adjust resources accordingly.
- Explain the need to establish and implement best practices, which are:
  - Methods or techniques that have consistently shown results superior to those achieved with other means
  - Used as benchmarks
  - Variable and change from asset to asset

Slide 30 Identify Interdependencies between Infrastructures
▪ Relationship between infrastructures ▪ Geographic proximity ▪ Feasibility
Graphic Description: Aerial view of a dam next to a high bridge across a canyon

- Explain that the following considerations will help to identify priorities and solutions:
  - Relationship between infrastructures
  - Geographic proximity
  - Feasibility
- Tell participants to consider cost-effective solutions for vulnerabilities.
  - Explain that considering relationships between infrastructures that are different but related can provide a cost-effective solution to reduce the overall effect of an attack. For example:

  - Energy production — depends on transportation and information technology networks
  - Transportation — depends on energy and information technology networks
  - Information technology networks — depend on energy
  - Because of these interdependencies, an attack on one segment could have a debilitating effect on other infrastructures.
- Explain that geographic locations where a number of critical assets of one or more infrastructure are located together might warrant priority. For example:
  - One of the most significant findings associated with the 2001 attacks on the United States' World Trade Center was that the area housed a number of assets associated with banking and finance, electric power, and telecommunications, some of which had no backup assets located elsewhere.
  - In this case, the losses associated with these assets were fairly localized to lower Manhattan, in New York City, and the services were quickly reconstituted elsewhere.
  - However, those responsible for ensuring services recognized the value of knowing the proximity of critical assets.
- Explain that another way to prioritize with regard to allocating resources, is to focus on:
  - Infrastructure that is entirely owned and operated by government, such as military installations and federal agencies
  - Private or local infrastructure depended on to carry out official responsibilities, such as communication companies that provide the infrastructure for messages pertaining to public safety concerns
  - Private or local infrastructure with government relationships such as privately owned utility companies, financial institutions, and hospitals
- Tell participants that the implication is that infrastructure not connected to the government must take primary responsibility for addressing its own vulnerabilities and the possible effects of an attack.
- Explain that prioritization is critical because limiting the number of infrastructures under study without proper analysis might miss a dangerous vulnerability.

Slide 31 Discussion Question
▪ Why is the evaluation of a critical infrastructure's components an important part of the vulnerability analysis?
Graphic Description: No Graphic

- Ask participants: **Why is the evaluation of a critical infrastructure's components an important part of the vulnerability analysis?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Allows security managers to ensure that resources and time are focused on the appropriate facilities*
  - *Avoids wasting time and resources*
  - *Ensures security countermeasures are implemented on most important facilities*

- Explain that the next section will cover the methodology for gathering the information for these components.

Slide 32 Methodology for Gathering Information on Facilities

- This section will cover:
  - Stage 1: Planning
  - Stage 2: Data review
  - Stage 3: Site visit
  - Stage 4: Information evaluation

Graphic Description: No Graphic

- Explain that the methodology for gathering the information needed for the critical infrastructure component evaluation includes the following stages:
  1. Planning
  2. Data review
  3. Site visit
  4. Information evaluation
- Explain that employing a structured system for gathering data will ensure adequate and accurate information is gathered.
- **Note:** as you present the information, describe the component evaluation information you gathered from the host facility and the methodology you used to obtain the information from the host facility.
  - In the event you were not able to gather information about the host facility, describe how you would have applied the recommended methodology stages and what information you would have gathered, specific to the host facility.
  - After you describe the methodology you would use, you will also present samples of the information you gathered, if any, regarding the host facility.

Slide 33 Gathering Component Data — Stage 1: Planning (Workbook 5.1)

- Form a vulnerability analysis team:
  - Project manager
  - Security system technologist
  - Subject matter experts
- Make a data call:
  - Before site visit
  - Request information about site
- Schedule site visit — time and permission

Graphic Description: No Graphic

- Refer to **Workbook 5.1: Gathering Component Data**.
- Tell participants to refer to this document as you discuss the stages of the methodology.

- Explain that before performing the vulnerability analysis, security managers must do preliminary work to plan and execute a project strategy.
- Refer participants to **Figure 1** in **Workbook 5.1: Gathering Component Data.**
- Tell participants that this vulnerability analysis team diagram provides a visual representation of members to include on a vulnerability analysis team:
  - A project manager responsible for coordinating and assigning tasks as required
  - A security system technologist(s) who knows and understands in detail the types of security countermeasures that could be deployed at the site
  - A subject matter expert(s) who understand the threat analysis process
  - Additional subject matter experts from the site, such as a safety expert, to ensure that all critical assets are identified and critical infrastructure components are evaluated appropriately
- Explain that it is critical that subject matter experts from the selected facility be a part of the vulnerability analysis team to:
  - Provide accurate data about the site and specific operations
  - Expedite the vulnerability analysis team's ability to arrange site tours
  - Identify individuals to be interviewed
  - Assist in completing the analysis
- Explain what you would do during the planning stage of the process for assessing the critical infrastructure components of the host facility.
- Explain that prior to arranging the site visit, the vulnerability analysis team's project manager should request a data call to request information about the site.
- Tell participants that this call for information helps the subject matter experts and project manager determine the types of questions to ask while on-site and provides details on security systems and critical assets. This call should be made 30 days prior to the site visit to provide time to review the data.
- Define **data call**: To request information about the site prior to actually performing the site visit.
- Refer participants to the **Data Call Checklists** section **Workbook 5.1: Gathering Component Data** for a detailed review of the data call checklists for planning elements from each critical infrastructure component category:
  - Physical conditions
  - Facility operations
  - Facility policies and procedures
  - Regulatory requirements
  - Safety considerations
  - Legal considerations
- Explain the process of scheduling a site visit with the critical infrastructure site point of contact.
  - Time is always a consideration in scheduling a site visit.
  - Depending on the critical asset, prior permission for a site visit may only need a phone call.
  - However, in some cases, advanced written permission may be required.

Slide 34 Discussion Question
▪ What other kinds of information would you want to obtain from the data call?
Graphic Description: No Graphic

- Ask participants: **What other kinds of information would you want to obtain from the data call?**
- Acknowledge responses. *Responses will vary.*
- Describe the information you would request and expect to receive from the host facility during this stage.

Slide 35 Gathering Component Data — Stage 2: Data Review (Workbook 5.1) 
▪ Review data call information ▪ Prepare questions for site visit ▪ Plan site visit
Graphic Description: Person holding a magnifying glass over data rising off the screen of a tablet

- Explain that the data review stage includes:
  - Reviewing data received from data call
  - Preparing questions for site visit
  - Planning the site visit, including time needed and team members available
- Explain that during the data review stage, the host facility sends the data call responses to the vulnerability analysis team for the project manager and experts on the team to review.
- Tell participants that from the review of the data call information, the vulnerability analysis team will prepare questions for the interview process and annotate information that may require clarification for reference during the site visit.
- Refer participants to the **Data Review Questions section** in **Addendum 5.2: Gathering Component Data**:
  - Physical conditions
  - Facility operations
  - Facility policies and procedures
  - Regulatory requirements
  - Safety considerations
  - Legal considerations
- Explain that the questions included are samples and actual questions are formulated based on the facility, data collected from the data call, and subsequent materials provided.
- Explain that at this point, the team should have already scheduled the site visit.
- Tell participants that planning the duration of the visit is dependent on the size of the facility visited and the number of vulnerability analysis team members available to attend.

- Explain what you would do during the data review stage of the process for assessing the host facility.
- Describe the information you might expect from the host facility during this stage and what you would do with the information.

Slide 36 Discussion Question
▪ Are there any other sample questions you would include in the list?
Graphic Description: No Graphic

- Ask participants: **Are there any other sample questions you would include in the list?**
- Acknowledge responses. *Responses will vary.*

Slide 37 Gathering Component Data — Stage 3: Site Visit
▪ Briefing to facility point of contact ▪ Tour, including: • All critical assets • Secondary critical assets • Security control center • Other specified areas ▪ Interviews to answer remaining questions
Graphic Description: Group of three people who appear to be on a touring a storage facility

- Define **secondary** critical assets: secure areas that are accessible only after entrance through a primary access controlled entry, including uninterrupted power supply and security control center, the heating and ventilation supply, switching rooms and build rooms.
- Explain the site visit:
  - **Briefing** — the site visit begins with a briefing to the facility point of contact and any site experts assisting in the review. During the briefing, the vulnerability analysis team focuses on the types of information needed as well as the interview schedule for the facility.
  - **Tour** — after the briefing, the vulnerability analysis team should receive a complete tour of the facility so that the information reviewed from the data call can be confirmed or irregularities observed and noted for future investigation. At a minimum, the tour should include:
    - All critical asset areas (such as operating facilities, the location of information technology infrastructure and classified data)
    - Secondary critical assets: secure areas that are accessible only after entrance through a primary access controlled entry, such as power generating capabilities and information systems rooms.
    - The security control center
    - Other areas as specified by the vulnerability analysis team

  - **Interviews** — after the tour, experts from the vulnerability analysis team and the site team proceed with the interviews, which are designed to solicit answers to questions formulated during the data review or during the site tour.
- Remind participants of the kinds of questions to ask for each component during the site visit. Refer to the addendum if needed.

Slide 38 Gathering Component Data Stage 4: Information Evaluation
▪ Determine data relevance ▪ Record in report
Graphic Description: Fingers typing on keyboard

- Explain what to do after the site visit, including:
  - Determine relevance of information — after gathering information, the vulnerability analysis team determines what is relevant based on their expertise.
  - Record in physical protection system report — the relevant information is recorded in the assessing critical infrastructure components section of the physical protection system report for reference as required.
  - Omit information that does not support a finding or observation during the site visit.
    - There may be dozens of regulatory requirements for the site, but only mention the ones pertaining to security in the report if there were no reportable regulatory issues. Even then, only certain regulations may be referenced if a finding occurs.
    - For example, the report may have a statement that says, "The facility security plan was shown to be within European Union (EU) regulations EU 1019-1020, with the exception of the requirement to conduct an annual evacuation drill, as listed in EU 1019B."
  - Explain what you would do during the information evaluation stage of the process for the host facility.

Slide 39 TeachBack Moment 
▪ How are critical infrastructure components used in a critical infrastructure assessment?
Graphic Description: No Graphic

- Conduct a TeachBack moment to assess how well the participants understand the content presented in this section of the module.
- Ask participants: **How are critical infrastructure components used in a critical infrastructure assessment?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Used to identify critical assets to protect*
  - *Assists in the efforts to prioritize actions and resources to protect the asset*
  - *Allows for limited resources to be used more efficiently*

- Tell participants that now they will have the chance to practice evaluating critical infrastructure components for a fictional location, the National Ministries Building.

Topic: Threaded Exercise Introduction and Part 1 — National Ministries Building	**100 Minutes**

Enabling Learning Objective:
- Evaluate the critical infrastructure components for a critical asset in a given scenario.

Slide 40 Threaded Exercise Introduction and Part 1

- Purpose: to evaluate the critical infrastructure components of the National Ministries Building
  - Duration: 90 minutes (70-exercise; 20-debrief)
  - Group composition: table groups
  - Debrief: presentation and discussion

Graphic Description: No Graphic

Slide 41 National Ministries Building Complex Map

- *No Text*

Graphic Description: National Ministries Building map and buildings

- Refer to facilitator **Threaded Exercise Workbook Introduction and Part 1 — National Ministries Building Answer Key** for answers to Part 1 of the National Ministries Building Exercise.
- Refer participants to **Threaded Exercise Workbook Introduction and Part 1 — National Ministries Building**.
- Explain that each group will be functioning as a vulnerability analysis team.
- Assign an interpreter to each group if needed.
- Discuss the introduction and directions for **Threaded Exercise Workbook Introduction and Part 1 — National Ministries Building, 1.1: Conduct Vulnerability Analysis Team Assignment**.
  - Discuss experience level of the team members.
  - Appoint a project manager and assign roles to the remaining members:
    - Security system technologist(s)
    - Subject matter experts
  - Use Table 1: Vulnerability Analysis Team Assignments to list the name and role of each team member.
  - Teams have 10 minutes to complete this segment of the exercise.
- Discuss the directions for **Threaded Exercise Workbook Part 1 — National Ministries Building, 1.2: Prepare for the Data Call**.
  - Write down, in the space provided, the types of information the vulnerability analysis team would like to have.
  - Refer to the information from Addendum 5.2: Gathering Component Data to help teams identify what they need.

  - Teams have 15 minutes to complete this segment of the exercise.
- Discuss the directions for **Threaded Exercise Workbook Part 1 — National Ministries Building, 1.3: Complete a Review of Data Call Information**.
  - Read through the appropriate sections.
  - Discuss the types of information received.
  - In the space provided:
    - List all the relevant information.
    - Identify any missing information.
    - List any needed clarifying information.
  - Teams have 30 minutes to complete this segment of the exercise.
- Discuss the directions for **Threaded Exercise Workbook Part 1 — National Ministries Building, 1.4: Develop Questions for Each Critical Infrastructure Component**.
  - Prepare four questions for each of the critical infrastructure components listed.
  - Write the questions in the space provided.
  - Teams will have 15 minutes to write the questions.
- Tell all teams they should be prepared to present their information to the class.
- During the exercise, all facilitators should circulate in the classroom to answer questions.
- At the completion of the exercise, to debrief, the facilitators will call on each team to present on a different component.
  - For example, have team 1 present on physical conditions, team 2 present on facility operations, and so on.
  - After a team reports on a component, ask whether any of the other teams have additional comments for that component.
- After the participants complete Part 1 of the exercise, conclude the module with the module summary.

Topic: Module Summary	**15 Minutes**

Slide 42 Module Summary
▪ Critical infrastructure assessments ▪ Critical infrastructure components
Graphic Description: No Graphic

- Summarize the module by reminding participants of the following main points:
- **Critical infrastructure assessments:**
  - Avoid wasting resources
  - Protect critical assets
  - Conduct vulnerability analysis on the right facility
  - Gather data for the critical infrastructure components:
    - Environment and physical conditions
    - Facility operations
    - Facility policies and procedures

    - Regulatory requirements
    - Safety considerations
    - Legal considerations
- **Critical infrastructure components:**
    - Methodology for gathering the information for the critical infrastructure components:
        - Plan
        - Request and review data
        - Conduct the site visit
- Ask whether there are any questions about the contents of this module.
- Explain that *Module 6: Critical Infrastructure Assets* explains the next step in the vulnerability analysis process and provides further detail on how to prioritize assets and conduct a target threat analysis.

This Page Intentionally Left Blank.