MODULE 6: CRITICAL INFRASTRUCTURE ASSETS

Day: 3 **Time:** 4.0 Hours **Level of Understanding:** Analysis

Instructional Strategies:	▪ Lecture ▪ Large-Group Discussion ▪ Small-Group Exercise ▪ TeachBack Moment
Module Equipment/Facilities:	▪ Standard Classroom Setup ▪ Addendum 6.1: Critical Asset Identification Activity Answer Key ▪ Threaded Exercise Workbook Part 2—National Ministries Building Answer Key ▪ National Ministries Building Complex Map
Participant Materials/Handouts:	▪ Handout 6.1: Critical Asset Identification Activity ▪ Workbook 6.1: Undesirable Consequences of Critical Asset Loss Analysis ▪ Workbook 6.2: Threat Spectrum Matrix ▪ Threaded Exercise Workbook Part 2 — National Ministries Building

Terminal Learning Objective

By the end of this module, you will be able to analyze critical infrastructure assets in order to prioritize them for protection.

Introduction

In the previous module, you discussed how an assessment of critical infrastructure components forms the basis of the vulnerability analysis. In this module, you will continue with the next step of the vulnerability analysis by discussing the procedures for identifying critical infrastructure assets (people, processes, information, and equipment) and the methods used to prioritize these critical assets for protection. This will help you determine **what** to protect, rather than **how** to protect it. As part of your vulnerability analysis, you will also examine the critical assets from the perspective of a terrorist, who would consider critical infrastructure assets to be potential **targets**.

Once you identify and prioritize the assets as potential terrorist targets, it may still be difficult to provide the same level of protection for each asset. To address this issue, you must consider the consequences associated with the loss of each asset based on a defined threat. You will use matrices to analyze the range of potential threats (threat spectrum), including the consequence of the loss and the probability (likelihood) of attack. After you have identified the potential terrorist targets, you can then conduct a threat analysis, which

will provide the foundation required to evaluate each critical infrastructure's physical protection system.

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 Assets	▪ Define terms and categories relating to critical assets.	60 minutes
Undesirable Consequences of Critical Asset Loss Analysis	▪ Determine the negative consequences of a terrorist attack on critical assets.	85 minutes
Threaded Exercise Part 2 — National Ministries Building	▪ Prioritize assets for a given critical infrastructure.	110 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 analysis	The complete description of the types of assets under each sector or category of critical infrastructure and the identification of undesirable consequences for each type
Critical asset	Any people, information, processes, and equipment that must be protected to prevent an undesired consequence from occurring
Probability of occurrence	The likelihood that a terrorist will attack or an undesirable event will happen
Threat	Natural or man-made occurrence, individual, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property
Threat analysis	Product or process of identifying or evaluating entities, actions, or occurrences, whether natural or man-made, that have or indicate the potential to harm life, information, operations, the environment, and/or property
Threat spectrum	The range of potential threats to a critical infrastructure asset

Key Term	Description
Threat spectrum matrix	A table that visually illustrates the relationships between consequence, level of consequence, and probability of occurrence

Topic: Module Introduction 5 Minutes

Slide 1 Critical Infrastructure Assets

- 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.

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 before beginning the module.

Slide 2 Module Objective

- By the end of this module, you will be able to analyze critical infrastructure assets in order to prioritize them for protection

Graphic Description: No Graphic

- Briefly discuss the terminal learning objective.
- Highlight the main topics to be presented:
  - Critical Assets
  - Undesirable Consequences of Critical Asset Loss Analysis
  - Threaded Exercise — National Ministries Building Part 2

Slide 3 PPS Diagram

- *No Text*

Graphic Description: PPS diagram with Identify Critical Infrastructure Assets highlighted in yellow

- Remind participants that *Module 2: Introduction to Critical Infrastructure Security and Resilience* covered the first step of Phase 1 of the Physical Protection System Diagram: Identify Critical Infrastructure.

- Remind participants that *Module 5: Critical Infrastructure Components* covered the second step in Phase 1 of the Physical Protection System Diagram: Assess Critical Infrastructure Components.
- Explain that in this module, participants will view the third and final step of Phase 1 of the Physical Protection System Diagram: Identifying Critical Infrastructure Assets.
- Refer participants to the Physical Protection System Diagram for a visual representation of this step.

Topic: Critical Assets	**60 Minutes**

Enabling Learning Objective:
- Define terms and categories relating to critical assets.

Slide 4 Critical Assets
▪ Any people, information, processes, and equipment that must be protected to prevent an undesired consequence from occurring
Graphic Description: No Graphic

- Define **critical asset:** any people, information, processes, and equipment that must be protected to prevent an undesired consequence from occurring.
- Remind participants that in *Module 5: Critical Infrastructure Components,* they learned to analyze the various characteristics of critical infrastructure in order to better define vulnerabilities for each category of critical infrastructure.
- Explain that in this module participants will examine the facilities listed in the last module to identify the critical assets belonging to those facilities.

Slide 5 Categories of Critical Assets (1 of 2)
▪ People — dignitaries, government leaders, and officials or individuals in critical mission-specific positions ▪ Information — classified documents, reports, or other proprietary data
Graphic Description: Guests checking in at a hotel

Slide 6 Categories of Critical Assets (2 of 2)
▪ Processes — backup and storage of data processing materials and special analytical programs ▪ Equipment — data processing equipment, military weapons, computers, and vehicles
Graphic Description: Computer screen with open file folder and closed folders with padlocks

- Explain that critical assets will fall into one of these four categories:
  - **People:** dignitaries and other very important persons, such as government leaders and officials or individuals in critical mission-specific positions (scientists, highly skilled and trained military personnel, or engineers)

- **Information:** classified documents, reports, or other proprietary data
- **Processes:** backup and storage of data processing materials and special analytical programs, as well as other functional processes that may not be automated
- **Equipment:** data processing equipment, military weapons, computers (may belong to both equipment category and processes category), and vehicles

Slide 7 Discussion Question
▪ Thinking back to the facilities listed in *Module 5: Critical Infrastructure Components*, what types of critical assets might belong to those facilities?
Graphic Description: No Graphic

- Ask participants: **Thinking back to the facilities listed in *Module 5: Critical Infrastructure Components*, what types of critical assets might belong to those facilities?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Individuals in leadership positions*
  - *Machinery, computer, and other technology-related equipment*
  - *Classified information*
  - *Specialized processes both automated and nonautomated*
  - *Back-up power or other public utility systems, security systems (equipment, processes, and personnel)*
  - *Ability to grow produce to feed the country*
  - *Specialized equipment designed to defend the nation*

Slide 8 Critical Asset Identification
▪ Identify all critical assets to prepare for **asset analysis** ▪ Identification must occur before prioritizing critical assets for protection
Graphic Description: Downtown area with large office buildings, bridges, and highways

- Define **asset analysis:** the complete description of the types of assets under each sector or category of critical infrastructure and the identification of undesirable consequences for each type.
- Explain that identifying all critical assets is necessary before conducting an asset analysis.
- Tell participants that critical asset identification must occur before prioritizing critical assets for protection can begin.

Slide 9 Critical Asset Identification Activity (Handout 6.1)

▪ Purpose: to identify critical assets for assigned facilities
  • Duration: 30 minutes (20-activity; 10-debrief)
  • Group composition: table groups
  • Debrief: large-group discussion

Graphic Description: No Graphic

- Refer participants to **Handout 6.1: Critical Asset Identification Activity**.
- Assign each team four facilities so all sixteen facilities are assigned (one team will have the example in the first row of the table, there is light shading in the addendum to help distinguish the four sets).
- Discuss the activity directions provided in the addendum:
  - Your facilitators will assign your team four facilities.
  - Locate your team's four assigned critical infrastructure facilities in *Table 1: Critical Asset Identification Matrix*.
  - For your assigned facilities, provide specific examples of assets for all four categories of critical assets (people, information, processes, and equipment).
  - Write your answers in the spaces provided.
  - Be prepared to share your answers with the class.
- Tell participants the first row is an example.
- Explain that although participants may not be able to identify a critical asset for every category, they should list as many assets as possible.
- Encourage participants to refer to the slides titled Critical Assets for examples of critical assets.
- Allow 20 minutes to complete this activity.
- Allow 10 minutes for the teams to read their answers for each critical infrastructure sector.
- After the completion of the activity, be sure to ask participants whether they have any questions about identifying critical assets or anything else covered thus far.
- Tell participants that the next section discusses how to prioritize assets.

Topic: Undesirable Consequences of Critical Asset Loss Analysis — 85 Minutes

Enabling Learning Objective:
- Determine the negative consequences of a terrorist attack on critical assets.

Slide 10 Protecting Critical Assets

- Cannot protect all critical infrastructure assets
- Prioritize all critical assets according to their importance
- Analyze critical assets to determine which to protect

Graphic Description: No Graphic

- Explain that it is not possible or practical to protect all of the critical assets of all a nation's or region's critical infrastructure assets — not even all the assets of a particular facility can be protected.
- Explain that, because of this, participants must prioritize all assets according to their importance by conducting an undesirable consequences of critical asset loss analysis.
  - The prioritization of assets involves weighing the consequences of loss against the probability of a specific threat.

  - The three-step prioritization process is the undesirable consequences of critical asset loss analysis presented in the next few slides.
- Tell participants this analysis will help facility managers decide which critical assets to protect.

Slide 11 Undesirable Consequences of Critical Asset Loss Analysis (Workbook 6.2)

- The steps are:
  1. Specify the undesirable consequences of loss for each critical asset
  2. Determine the levels (high, medium, low) of the undesirable consequences of loss for each asset
  3. Determine the probability of occurrence of undesirable events

Graphic Description: No Graphic

- Tell participants the next section presents each step of the analysis.
- Tell participants that as you present each step of the undesirable consequences of critical asset loss analysis, you will first review the items on the slides to explain the steps and then refer to various sections within the addendum.
- Explain that by discussing the steps in this manner and by using an example facility, participants will get a better understanding of how to complete the analysis.
- Refer participants to **Workbook 6.2: Undesirable Consequences of Critical Asset Loss Analysis,** then to *Table 1: Asset Protection Decision Matrix — Critical Asset Identification*.
- Explain that participants should assume they have already identified the critical assets of the water treatment facility that appear in the first column of the table.
- Explain that while only one asset per category appears in the addendum, participants should list all assets when using this table in the future to conduct their own analysis.

Slide 12 Specify the Undesirable Consequences of Loss for each Critical Asset (1 of 2)

- Define the anticipated negative effects from a specific type of **threat**:
  - Terrorist attack
  - Natural disaster
  - Biochemical attack
  - Other threat

Graphic Description: Aftermath of car bomb

- Define **threat**: natural or man-made occurrence, individual, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.
- Explain that the steps for deciding which critical assets to protect begin with specifying the undesirable consequences of loss for each critical asset you have identified.
- Explain that to do this, participants must first define the anticipated negative effects from a specific type of threat, for example, terrorist attack, natural disaster,

biochemical attack, vandalism, theft, criminal activities, or other threats, like a cyber-attack.

Slide 13 Specify the Undesirable Consequences of Loss for each Critical Asset (2 of 2)

- Consequence measure may be classified as a:
  - Loss of tangibles (revenue, life, or property)
  - Loss of intangibles (reputation)
  - Combination of tangibles and intangibles
- Identify sets of critical assets
- Consequence measure establishes consistency among assets

Graphic Description: No Graphic

- Explain that the consequence measure may be a loss of tangibles (loss of revenue, life, or property), loss of intangibles (damaged reputation or community trust), or a combination of these.
- Explain that participants should specify undesirable consequences of loss for each critical asset they identify, as well as for sets of critical assets. For example, if participants are analyzing an electric power facility, the set of critical assets that comprises this facility might include:
  - Commercial power system
  - Emergency generator system
  - Uninterrupted power supply batteries
    - For example:
      - If a facility-wide bombing destroys all three critical assets belonging to this set, the undesirable consequence of loss may be interruption of power to all areas serviced by the electric power facility.
      - If the bombing was limited to only the commercial power system, the emergency generator system and the universal power supply batteries would mitigate area-wide power loss — this scenario would alter the overall consequence of loss.
- Explain that the consequence measure must establish consistency among assets to allow for relative ranking of the consequences, which occurs later in the process, for example:
  - When analyzing various government buildings with varying employee populations, each building's population may relate to a potentially different consequence measure.
  - Buildings with less than 200 employees may be measured differently than buildings with 200–500 employees.

Slide 14 Undesirable Consequences of Loss Examples (1 of 2)

- Loss of life
- Theft of material or information
- Environmental damage
- Interruption of critical utilities

▪ Degraded business operations ▪ Workplace violence
Graphic Description: Casualty being moved to hospital

- Discuss the examples of undesirable consequences of loss:
  - **Loss of life** due to detonation of an improvised explosive device
  - **Theft of material or information** that could affect the safety of local citizens, for example nuclear material being dispersed in a crowd
  - **Environmental damage** due to release of hazardous material by theft or sabotage
  - **Interruption of critical utilities** such as water, power, or communications services
  - **Degraded business operations** due to structural, inventory, or neighborhood damage or customer decrease due to damage or fear
  - **Workplace violence**, extortion, or blackmail

Slide 15 Undesirable Consequences of Loss Examples (2 of 2)
▪ Building damage or collapse ▪ Equipment damage or destruction ▪ Damage to reputation ▪ Damage to national security ▪ Legal liability ▪ Disruption to economy
Graphic Description: Construction equipment area blocking road

  - **Building damage or collapse** from a propelled rocket attack by a terrorist
  - **Equipment damage or destruction** by saboteurs gaining unlawful access to a critical infrastructure facility
  - **Damage to reputation** by attacking a government monument that represents an icon for the nation
  - **Damage to national security** by an insider divulging classified information to a terrorist organization
  - **Legal liability** associated with failure to protect individuals from a terrorist attack in a public venue such as a mall or theater
  - **Disruption to economy** caused by a massive computer intrusion incident effecting the country's financial institutions
- Refer participants to **Addendum 6.2: Undesirable Consequences of Critical Asset Loss Analysis, Step 1: Specify Undesirable Consequences of Critical Asset Loss,** then to *Table 2: Asset Protection Decision Matrix — Undesirable Consequences*.
- Explain that this table illustrates how to list undesirable consequences of loss.
- Explain the following details of the examples shown in *Table 2: Asset Protection Decision Matrix — Undesirable Consequences:*
  - The consequences of loss for each critical asset listed in the second column.
  - Only one consequence of loss is shown for each related critical asset; participants should list all undesirable consequences of loss when using this table in the future to conduct their own analysis.

- The remaining columns of Table 2 will be completed as the other steps of the undesirable consequences of critical asset loss analysis process are covered in upcoming sections.

Slide 16 Determine Levels of Undesirable Consequences (1 of 5)
▪ A decision-making process that relies on knowledge about the importance of each critical asset ▪ When evaluating: • People assets: know the number of people and their expertise and skills
Graphic Description: No Graphic

Slide 17 Determine Levels of Undesirable Consequences (2 of 5)
• Equipment and process assets: • Know criticality of specific pieces of equipment and processes • Know about availability of backup equipment, processes, and systems
Graphic Description: Helicopter in field

- Tell participants that once they have specified all undesirable consequences of loss for each critical asset, they must then determine the levels of the undesirable consequences of loss for each critical asset.
- Explain that determining levels for the undesirable consequences of loss involves a decision-making process that relies on knowledge about the importance of each asset, for example when evaluating:
  - People assets, knowing important factors such as the total number of people who are vulnerable, as well as expertise and skill sets of those people
  - Equipment and process assets:
    - Knowing the criticality of the specific piece of equipment and the specific process
    - Knowing whether or not backup equipment is available and whether backup processes and systems are already established

Slide 18 Determine Levels of Undesirable Consequences (3 of 5)
▪ To make decisions about consequences: • Define all the negative effects of a specific threat's occurrence • Compare negative effects with all identified consequences of loss • Assign levels to the undesirable consequences of loss • Compare all loss levels to each other
Graphic Description: No Graphic

- Explain that the decision-making to determine levels of undesirable consequences should include:
  - Defining all possible negative effects of a specific threat's occurrence
  - Comparing those negative effects with all identified consequences of loss

  - Assigning levels to the undesirable consequences of the loss
  - Comparing all consequences of loss levels to each other
- Provide examples from your own experience as appropriate for making these decisions.

Slide 19 Determine Levels of Undesirable Consequences (4 of 5)
▪ Establish consequence levels by using a qualitative scale to determine undesirable consequences of loss as: • High — example: loss of life • Medium — example: moderate financial loss due to industrial espionage • Low — example: damage to a critical asset's reputation
Graphic Description: No Graphic

- Explain the qualitative scale and examples shown on the slide to establish consequence levels.
  - This is only one type of example.
  - Participants may develop their own scale using a numeric scale, or add categories such as "very high" or "very low" to the scale.
  - Keep the scale and metric simple.

Slide 20 Discussion Questions
▪ What are examples of high consequences of loss? ▪ What are examples of medium consequences of loss? ▪ What are some examples of low consequences of loss?
Graphic Description: No Graphic

- Ask participants the following discussion questions:
  - **What are examples of high consequences of loss?**
  - Acknowledge responses. *If not provided by participants, add the following:*
    - *Loss of life*
    - *Workplace violence*
    - *Environmental damage*
    - *Legal liability*
  - **What are examples of medium consequences of loss?**
  - Acknowledge responses. *If not provided by participants, add the following:*
    - *Equipment destruction*
    - *Building collapse with no casualties*
    - *Damage to national security*
    - *Degraded business operations*
  - **What are some examples of low consequences of loss?**
  - Acknowledge responses. *If not provided by participants, add the following:*
    - *Interruption of critical utility service with immediate backup system availability*
    - *Theft of material or information*
    - *Equipment damage*

- *Building damage*

Slide 21 Determine Levels of Undesirable Consequences (5 of 5) (Workbook 6.1)

- Assigning levels:
  - Helps determine overall effects
  - Requires communication between analysts
  - Provides rationale for levels
- Comparing all consequences of loss levels helps prioritize:
  - Critical infrastructure
  - Security upgrades

Graphic Description: No Graphic

- Explain that assigning levels to the undesirable consequences of loss:
  - Helps to determine the overall effects of the event
  - Requires dialog and communication among and agreement between analysts
- Explain that comparing all consequences of loss levels helps prioritize:
  - The most critical infrastructure
  - Where security upgrades may be allocated first
- Refer participants to **Workbook 6.1: Undesirable Consequences of Critical Asset Loss Analysis, Step 2: Determine Levels of Undesirable Consequences of Critical Asset Loss**, then to *Table 3: Asset Protection Decision Matrix — Determine Levels of Undesirable Consequence* and explain the following details of the examples shown in Table 3.
  - The third column illustrates the levels of undesirable consequences of loss.
  - This is the same qualitative scale of high, medium, and low.
  - The levels depend on circumstances related to the specified consequences of loss.
    - The interruption of critical water services is a low level of consequence in this example because an immediate backup system is available.
    - If a backup system were not available, the level could be medium or high.

Slide 22 Determine Probability of Occurrence (1 of 2)

- The likelihood that a terrorist will attack or an undesirable event will happen
- A complex process that must be conducted in coordination with a complete threat analysis

Graphic Description: No Graphic

- Define **probability of occurrence**: the likelihood that a terrorist will attack or an undesirable event will happen.
- Define **threat analysis:** a product or process of identifying or evaluating entities, actions, or occurrences, whether natural or man-made, that have or indicate the potential to harm life, information, operations, the environment, and/or property.

- Explain that determining probability of occurrence is a complex process that relies on the complete threat analysis information participants will discuss in *Module 10: Analyzing the Threat*.

Slide 23 Determine Probability of Occurrence (2 of 2) (Workbook 6.1)

- Examine historical records and information obtained during threat analysis:
  - Review previous reports regarding attacks against the facility
  - Consult terrorist trend experts to gather information about current terrorist attack operations
- Determine the level of probability using the scale of high, medium, and low

Graphic Description: No Graphic

- Explain how probability of occurrence is determined by examining historical records and other threat analysis data, using the water treatment plant example as follows:
  - Review previous reports regarding attacks against the water facility or similar facilities, if available.
  - Ask for the assistance of terrorist trend experts to gather information about current terrorist attack operations against critical public utility facilities (either on a national or global level or both).
- Explain that the following qualitative scale examples are only a reference point so that participants can start thinking about the variables and conditions that would affect how they would personally rate the probability of occurrence for certain events:
  - **High** — characterized by previous attempts and intelligence reports suggesting that attempts have been made, suggesting the possibility of future attacks
  - **Medium** — characterized by the possibility of attack but no real intelligence or evidence of attack , suggesting an attack may or may not be likely
  - **Low** — characterized by no previous attempts and no intelligence reports of attempted attacks, suggesting no future attacks
- Emphasize that the probability level is dependent upon the circumstances related to the specified consequences of loss.
- Explain that in this example, using the same scale of high, medium, and low helps provide consistent comparisons.
  - Other scale systems can be created, for example very low, low, medium, high, and very high — but each scale must be clearly defined from the beginning of the analysis.
  - Scale systems must not be mixed because it might skew the results of the comparisons.
- Refer participants to **Addendum 6.2: Undesirable Consequences of Critical Asset Loss Analysis, Step 3: Determine Probability of Occurrence of Undesirable Events**, then to the additional examples shown in *Table 4: Asset Protection Decision Matrix — Probability of Occurrence*.
- Tell participants that for the purposes of this module, the levels of probability of occurrence are already completed based on hypothetical threat analysis information that is presented in parentheses next to the assigned level of high, medium, or low.

Slide 24 Discussion Question
▪ Based on Table 4, and what you currently know about the probability of occurrence in your nation today for each undesirable consequence listed in column 2, what probability level determinations can you make?
Graphic Description: No Graphic

- Ask participants: **Based on Table 4, and what you currently know about the probability of occurrence in your nation today for each undesirable consequence listed in column 2, what probability level determinations can you make?**
- Acknowledge responses.
  - **Note**: Emphasize that participants should use their best collective judgment (based on personal knowledge or professional expertise) when determining probability of occurrence levels, since they do not have threat analysis information available at this time.
  - This is an open-ended question with many possible answers and not intended for debate.
- Ask participants whether they have questions about the undesirable consequences of critical asset loss analysis process or anything covered thus far.
- Tell participants that an undesirable consequences of critical asset loss analysis yields a large amount of information about the critical assets comprising a given facility.
- Tell participants that they will use this collected information to complete the threat spectrum matrix that is presented in the next section.

Slide 25 Threat Spectrum Matrix (1 of 6)
▪ A table that visually illustrates the relationships between consequence, level of consequence, and probability of occurrence ▪ A clear format to analyze and quickly see relationships between collected information
Graphic Description: No Graphic

- Define the following terms:
  - **Threat spectrum:** the range of potential threats to a critical infrastructure asset
  - **Threat spectrum matrix:** a table that visually illustrates the relationships between consequence, level of consequence, and probability of occurrence
- Explain that a threat spectrum matrix is a quick way to provide a visual comparison and evaluation between consequence, level of consequence, and probability of occurrence for all identified critical assets for a given facility.

Slide 26 Threat Spectrum Matrix (2 of 6)
▪ Presents risks to a facility across a threat spectrum at various consequence levels ▪ A completed matrix helps asset selection for protection ▪ Any asset with a high consequence and high probability level requires the highest priority for protection
Graphic Description: Rooftop units on a building

Slide 27 Threat Spectrum Matrix (3 of 6)

- Any asset with a low consequence and low probability level requires the lowest priority for protection
- The completed matrix may be used later in physical protection system design, when determining the allocation of resources

Graphic Description: No Graphic

- Explain that using this matrix helps to determine the risk to a facility across a threat spectrum and at varying consequence levels.
- When the matrix is complete, participants can select assets to protect, based on results of the matrix.
- The matrix is also valuable later during physical protection system design, when determining the allocation of resources — physical protection system design will be covered in *Module 14: Security Inspection and Validation*.

Slide 28 Threat Spectrum Matrix (4 of 6) (Workbook 6.2)

- *No Text*

Graphic Description: Figure 1: Threat Spectrum Matrix Format from addendum

Slide 29 Threat Spectrum Matrix (5 of 6) (Workbook 6.2)

- Consequences level scale — vertical axis
- Probability of occurrence scale — horizontal axis
- Parameters remain fixed for critical assets within a specific facility
- Qualitative scale must also remain fixed

Graphic Description: No Graphic

- Refer participants to **Workbook 6.2: Threat Spectrum Matrix, Introduction,** and *Figure 1: Threat Spectrum Matrix Format*.
- Explain the following details about the threat spectrum matrix from the addendum:
  - Consequences level scale — vertical axis
  - Probability of occurrence scale — horizontal axis
  - Parameters remain fixed when analyzing critical assets within a specific facility
  - The decision to use a qualitative scale, once made, must also remain fixed

Slide 30 Threat Spectrum Matrix (6 of 6) (Workbook 6.2 6.3)

- *No Text*

Graphic Description: Figure 2: Completed Threat Spectrum Matrix from addendum

- Explain that adding the information from Table 4 of Addendum 6.2 to complete the threat spectrum matrix would yield the following probability of occurrence levels:
  - **Loss of life** (terrorist bomb explosion) — high

  - **Damage to national security** (theft of diagram) — low
  - **Interruption of critical facilities** (bomb in control room) — high
  - **Environmental damage** (hazardous material) — medium
- Draw an empty threat spectrum matrix on a white board or flip-chart paper, including the labels for consequences and probability.
- Ask a representative from each table group to enter information for one asset from *Table 4: Asset Protection Decision Matrix — Probability of Occurrence* into the appropriate cell:
  - **Loss of life:** enter in cell where high consequences of loss and high probability of occurrence intersect
  - **Damage to national security:** enter in cell where medium consequences of loss and low probability of occurrence intersect
  - **Interruption of critical facilities:** enter in cell where low consequences of loss and high probability of occurrence intersect
  - **Environmental damage:** enter in cell where high consequences of loss and medium probability of occurrence intersect
- Explain that when using the actual results from a threat analysis, participants would repeat this same process for all identified critical assets.
- Emphasize that several assets will often be listed in one cell; for example:
  - Loss of life is of high consequence and high probability
  - Several other assets may also have high consequence of loss and high probability of occurrence

Slide 31 Discussion Questions (Workbook 6.2)

- Where in the threat spectrum matrix would you expect to see the assets that require the highest priority for protection?
- Where in the threat spectrum matrix would you expect to see the assets with the lowest priority for protection?

Graphic Description: No Graphic

- Ask participants the following discussion questions:
  - **Where in the threat spectrum matrix would you expect to see the assets that require the highest priority for protection?**
  - Acknowledge responses. *If not provided by participants, the correct response is: in the cell indicating high consequence and high probability levels.*
  - **Where in the threat spectrum matrix would you expect to see the assets with the lowest priority for protection?**
  - Acknowledge responses. *If not provided by participants, the correct response is: in the cell indicating low consequence and low probability levels.*
- Emphasize that when there is **low** probability of occurrence of a specific threat against an asset but **high** consequence of loss for that same asset, participants must carefully evaluate the protection priority.

Slide 32 Community Engagement and Human Rights Discussion

- When determining the undesirable consequences, why is it important to engage with community representatives?

Graphic Description: No Graphic

- Lead a brief discussion related to human rights and community engagement. For example, ask participants: **When determining the undesirable consequences, why is it important to engage with community representatives?**
- Acknowledge response. *If not provided by participants, add the following:*
  - *Law enforcement may not know all of the particular consequences should an asset be destroyed*
  - *Law enforcement may not know all of the effects should an asset's capability to function be stopped*

Slide 33 TeachBack Moment

- What are the four categories of critical infrastructure assets?
- What are the steps to determine undesirable consequences of critical asset loss?
- What are some of the negative consequences of a terrorist attack on a critical infrastructure asset?

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 categories of critical infrastructure assets?**
- Acknowledge the participant responses. *If not provided by participants, add the following:*
  - *People*
  - *Information*
  - *Processes*
  - *Equipment*
- Ask participants: **What are the steps to determine undesirable consequences of critical asset loss?**
- Acknowledge the participant responses. *If not provided by participants, add the following:*
  - *Specify the undesirable consequences of loss for each critical asset*
  - *Determine the levels (high, medium, low) of the undesirable consequences of loss for each asset*
  - *Determine the probability of occurrence of undesirable events*
- Ask participants: **What are some of the negative consequences of a terrorist attack on a critical infrastructure asset?**
- Acknowledge the participant responses. *If not provided by participants, add the following:*
  - *Loss of life*
  - *Theft of material or information*

- *Environmental damage*
- *Interruption of critical utilities*
- *Degraded business operations*
- *Workplace violence*
- *Building damage or collapse*
- *Equipment damage or destruction*
- *Damage to reputation*
- *Damage to national security*
- *Legal liability*
- *Disruption to economy*

- Ask participants whether they have questions about anything covered thus far.
- Explain that participants will now apply what they have learned in this module to a continuation of the scenario that began in *Module 5: Critical Infrastructure Components.*

Topic: Threaded Exercise Part 2 — National Ministries Building	**110 Minutes**

Enabling Learning Objective:
- Determine the negative consequences of a terrorist attack on critical assets.

Slide 34 Threaded Exercise Part 2 — National Ministries Building

- Purpose: to prioritize consequences for a given critical infrastructure
  - Duration: 110 minutes (90-exercise; 20-debrief)
  - Group composition: table groups
  - Debrief: presentation and discussion

Graphic Description: No Graphic

Slide 35 National Ministries Building Complex Map

- *No Text*

Graphic Description: Map of National Ministries Building and surrounding buildings

- Refer to facilitator **Threaded Exercise Workbook Part 2 — National Ministries Building Answer Key** for answers to Part 2 of the National Ministries Building Threaded Exercise.
- Refer participants to **Threaded Exercise Workbook Part 2 — National Ministries Building**.
- Refer participants to the **National Ministries Building Complex Map** for a visual representation of the National Ministries Building complex.
- Tell participants they will work in the same teams established in *Module 5: Critical Infrastructure Components.*
- Discuss the introduction and directions for **Threaded Exercise Workbook Part 2 — National Ministries Building, 2.1: Identify Critical Infrastructure Assets and Loss Analysis**.

- Remind participants that in the previous module, each team initiated a data call to the National Ministries Building facility director requesting information on the building.
  - Ask participants the following discussion question: **Since the facility director did not provide specific information relating to critical assets, did your team request additional information regarding critical assets?**
  - Acknowledge responses.
- Emphasize the importance of requesting additional information when necessary.
- Explain that for the purposes of this exercise, assume a second request regarding critical assets was made and additional information was received.
- Discuss the exercise directions:
  - Review and discuss the Facility Director's Second Response Letter with their team.
  - Use the information presented in the letter to work with their team members to identify critical assets belonging to the National Ministries Building.
  - Use all the information that teams have received and compiled to this point to complete *Table 2: Undesirable Consequences of Critical Asset Loss Analysis.*
    - To complete column 1, document the critical assets they identified in the facility director's letter
    - To complete columns 2 and 3, assume that all undesirable consequences of critical asset loss are related specifically to the identified critical asset
    - To complete column 4, apply their team's best collective judgment (based on personal knowledge or professional expertise) when determining the probability of occurrence levels because the teams do not have threat analysis information available at this time
  - The teams will have 60 minutes to complete this segment of the exercise.
- Discuss the directions for **Threaded Exercise Workbook Part 2 — National Ministries Building, 2.2: Create Threat Spectrum Matrix**.
  - Discuss and complete *Table 3: Threat Spectrum Matrix — National Ministries Building* with their team.
  - Transfer information from Table 2 into the appropriate cells within the threat spectrum matrix.
  - Remind participants they may have several asset-related consequences of loss within any one given cell.
  - The teams will have 30 minutes to complete this segment of the exercise.
  - Each team should be prepared to share their completed threat spectrum matrix with the class.
- During both portions of the exercise, all facilitators should circulate in the classroom to answer questions.
- Emphasize that:
  - Discussion among team members is important
  - Presentation of a group's rationale for each rating is important in determining the threats and associated consequences
- At the completion of the exercise, the facilitators will choose one team to make a 10-minute presentation and explanation of its threat spectrum matrix.
- Explain that the team should focus primarily on the following two cells:

- High consequence and high probability
- Low consequence and low probability

Slide 36 Threaded Exercise Part 2 — Discussion Questions

- What influenced your decision regarding probability of occurrence levels?
- What additional information would you need to make more accurate decisions about probability of occurrence?

Graphic Description: No Graphic

- Allow 10 minutes for this discussion.
- Ask the presenting team the following discussion questions:
  - **What influenced your decision regarding probability of occurrence levels?**
  - Acknowledge responses. *If not provided by participants, add the following:*
    - *The team's personal knowledge of the threat and actual consequences of loss*
    - *In the absence of knowledge, the team made an educated guess*
    - *However, the team did recognize the potential error in their guess*
  - **What additional information would you need to make more accurate decisions about probability of occurrence?**
  - Acknowledge responses. *If not provided by participants, add the following:*
    - *Information from intelligence sources*
    - *Other historical data*
    - *Current information about potential attacks at other critical infrastructure facilities*

Topic: Module Summary — 10 Minutes

Slide 37 Module Summary

- Critical assets
- Undesirable consequences of critical asset loss analysis

Graphic Description: No Graphic

- Summarize the module by reviewing the following main points:
  - **Critical assets:**
    - People
    - Information
    - Processes
    - Equipment
  - **Undesirable consequences of critical asset loss analysis:**
    - Specify the undesirable consequences of loss for each critical asset
    - Determine the levels (high, medium, low) of the undesirable consequences of loss for each asset
    - Determine the probability of occurrence of undesirable events
    - Loss of life

- Theft of material or information
- Environmental damage
- Interruption of critical utilities
- Degraded business operations
- Workplace violence
- Building damage or collapse
- Equipment damage or destruction
- Damage to reputation
- Damage to national security
- Legal liability
- Disruption to economy

- Ask whether there are any questions about the contents of this module.

Explain that *Module 7: Cybersecurity* will discuss responses to cyber threats.