MODULE 10: ANALYZING THE THREAT

Day: 4, 5 **Time:** 4.5 Hours **Level of Understanding:** Analysis

Instructional Strategies:

- Lecture
- Large-Group Discussion
- Case Study
- Video
- Small-Group Exercise
- TeachBack Moment

Module Equipment/Facilities:

- Standard Classroom Setup
- Addendum 10.1: Sample Threat Analysis Statement Case Study Answer Key
- Workbook 10.2: Insider Threat Worksheet Activity Answer Key
- Workbook 10.3: Outsider Threat Worksheet Activity Answer Key
- Workbook 10.4: Estimating Likelihood of Attack Activity Answer Key
- Workbook 10.5: Preparing a Threat Analysis Statement Activity Answer Key
- Threaded Exercise Workbook Part 3 — National Ministries Building Answer Key
- National Ministries Building Complex Map

Participant Materials/Handouts:

- Workbook 6.2: Threat Spectrum Matrix
- Handout 10.1: Sample Threat Analysis Statement Case Study
- Handout 10.2: Washington Navy Yard Shooting Case Study
- Workbook 10.1: Analytical Thinking
- Workbook 10.2: Insider Threat Worksheet Activity
- Workbook 10.3: Outsider Threat Worksheet Activity
- Workbook 10.4: Estimating Likelihood of Attack Activity
- Workbook 10.5: Preparing a Threat Analysis Statement Activity
- Threaded Exercise Workbook Part 3 — National Ministries Building

Terminal Learning Objective

By the end of this module, you will be able to create a threat analysis statement for critical infrastructure.

Introduction

As you are already aware, terrorists use a variety of tactics and types of weapons to plan and implement their attacks. In this module, you will recognize the importance of analyzing terrorist threats and evaluating the range of potential threat that could cause damage to critical infrastructure assets (people, information, processes, and equipment).

A threat is an individual or group who may pose a wide range of threats to a facility. It even includes nonterrorist related events, such as an employee becoming violent in the workplace. Although the focus of this module will be on terrorist threats, you should be aware of the threat to security that various types of natural disasters may cause as you analyze the security of your critical infrastructure locations. Including disaster drills that cover all aspects of security including cybersecurity will prepare critical infrastructure personnel for threats posed by natural disasters.

This module will cover the information sources used in threat analysis, so that you have a better understanding of terrorist threat indicators, motivation, tactics, equipment, and weapons. Also included in this module is important information on the collection and analysis of data for the development of the threat analysis statement.

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
Purpose of the Threat Analysis	▪ Explain the importance of analyzing the threat.	55 minutes
Potential Adversary Threats	▪ Explain the types of potential adversary threats.	80 minutes
Information Sources about Potential Threats	▪ Describe sources of information used in analyzing a threat.	60 minutes
Threaded Exercise Part 3 — National Ministries Building	▪ Develop a threat analysis statement for a given critical infrastructure.	60 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
Access	The ability to gain entrance to asset
Adversary	An individual, group, organization, or government that conducts activities, or has the intention and capability to conduct activities, detrimental to a government or facility
Critical infrastructure assets	The resources (people, information, processes, and equipment) that support the operation of a critical infrastructure
Deceit	An overt act of trying to misinform someone to gain access
Diversion of materials	The unlawful movement or transfer of funds, information, or equipment
Force	An overt attempt to overcome a physical protection security system by violence
Sabotage	The deliberate and malicious destruction of property with the intent to cause harm to people, equipment, processes, and information with the intent to disrupt or stop operations of a facility
Stealth	An act of completing an adversarial task without being noticed, or going undetected
Terrorists	Individuals who unlawfully use force against persons or property to intimidate or coerce a government and its civil population to achieve a political or social objective
Theft	The unlawful possession of property, equipment, information, materials, or other valuable products; may also refer to unlawful diversion of funds or information

Topic: Module Introduction	**5 Minutes**

Slide 1 Analyzing the Threat
▪ 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: due to the length of this module (4.5 hours), consider having two facilitators prepared to teach different portions. This will provide the facilitator a break from extended teaching and the participants a break from listening to the same facilitator for each section.
- Note: be prepared to discuss a possible threat analysis statement for the host 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 and workbook participants will use during this module.
  - Explain that instructions for all exercises are included in the addendums and the workbook.
  - 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 create a threat analysis statement for critical infrastructure
Graphic Description: No Graphic

- Briefly discuss the terminal learning objective.
- Highlight the main topics to be presented:
  - Purpose of the Threat Analysis
  - Potential Adversary Threats
  - Information Sources about Potential Threats
  - Threaded Exercise Part 3 — National Ministries Building
- Ask participants whether they have any questions about anything covered this far in the course.

Slide 3 Physical Protection System
▪ *No Text*
Graphic Description: PPS diagram with Analyzing the Threat highlighted in yellow

- Point out on the slide where analyzing the threat appears on the diagram.

Topic: Purpose of the Threat Analysis	**55 Minutes**

Enabling Learning Objective:
- Explain the importance of analyzing the threat.

Slide 4 Purpose of the Threat Analysis
▪ Gather threat data ▪ Identify data sources ▪ Prepare threat analysis statement ▪ Establish physical protection system design requirements
Graphic Description: No Graphic

- Explain that the purpose of threat analysis is to:
  - Gather data on one or more threats
  - Identify data sources
  - Prepare threat analysis statement
  - Establish the physical protection system design requirements for their critical infrastructure
- Explain that the threat analysis may refer to a single threat or a spectrum of threats and may allow participants to determine the credibility of specific threats against a critical infrastructure.
- Tell participants that looking at **Workbook 6.2: Threat Spectrum Matrix** will assist them throughout this module.

Slide 5 Threat Analysis Statement (1 of 2)
▪ Identifies potential or credible threat capabilities ▪ Represents an assessment by informed and qualified people using available information
Graphic Description: Three men conducting threat assessment

- Remind participants of the definitions from *Module 6: Critical Infrastructure Assets*:
  - **Threat:** any indication, circumstance, or event with the potential to either damage or destroy an asset; also refers to an adversary's ability to undertake actions detrimental to a country's interests
  - **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 some organizations identify the threat in a single threat statement and others include it in a spectrum of potential threats.
  - Remind participants of the discussion about the threat spectrum in *Module 6: Critical Infrastructure Assets*.
  - Explain that in either case the threat or threat spectrum that they create is called the threat analysis statement.
  - Explain that organizations then use this statement in the various vulnerability analyses conducted across the organization.
- Explain the relationship between the threat analysis and the threat analysis statement: participants will convert the elements from the threat analysis into a narrative — the threat analysis statement — that will serve as a guide to developing security measures for the critical infrastructure.
- Explain that that the threat analysis statement may not represent the real threat.
- Emphasize that the threat analysis statement is information for official use only, available only to select individuals — treat the threat analysis statement as classified, sensitive, or proprietary data.

Slide 6 Threat Analysis Statement (2 of 2)
▪ Helps determine the basic requirements of a critical infrastructure's physical protection system ▪ Review and update as necessary
Graphic Description: No Graphic

- Explain that a threat analysis statement:
  - Enables security managers to understand the effects of a terrorist attack upon a particular critical infrastructure
  - Is an important means for physical protection system designers to determine the basic requirements of a critical infrastructure's physical protection system
- Explain that participants and their agencies should periodically review the threat analysis statement and make revisions and updates to it as needed.
- Provide an example from your own experience of how threat analysis statements have been used or overlooked in the past or use the example of the World Trade Center and Pentagon attacks in the United States on September 11, 2001:
  - Before the attacks on the World Trade Center and Pentagon, authorities had some indication an attacker may use a single airplane as a weapon.
  - They did not consider the possibility that attackers may use several airplanes as weapons, which turned out to be the real threat.
  - Security managers never considered the kind of coordinated multiple attack that occurred in the United States on that day.

Slide 7 Sample Threat Analysis Statement Case Study (1 of 3) (Handout 10.1)

- Purpose: to examine a sample threat analysis statement from a given case study
  - Duration: 30 minutes (20-reading; 10-discussion)
  - Group composition: table groups
  - Debrief: large-group discussion

Graphic Description: No Graphic

Slide 8 Sample Threat Analysis Statement Case Study (2 of 3) (Handout 10.1)

- Facility: nuclear power plant in Pelindaba, South Africa
- Specific threat: terrorist, radiological sabotage
- Credible threat: terrorist, theft, or diversion of special nuclear material

Graphic Description: Interior nuclear power plant

- Refer participants to **Handout 10.1: Sample Threat Analysis Statement Case Study**.
- Explain that each group will read the case study about the nuclear plant attack in South Africa and then answer discussion questions about the sample threat analysis statement.
- Tell participants to be prepared to answer large-group discussion questions regarding the case study.
- Allow 20 minutes for teams to read the case study and answer the questions in the addendum prior to the discussion.

Slide 9 Sample Threat Analysis Statement Case Study (3 of 3) (Handout 10.1)

- What critical information was not included in the sample threat analysis?
- What were the some of the significant points of the case study?
- What were some of the security countermeasure failures?

Graphic Description: No Graphic

- Tell participants that the sample threat analysis statement in **Handout 10.1: Sample Threat Analysis Statement Case Study** includes both a specific threat — identified as a terrorist, radiological sabotage — and a credible threat — identified as terrorist, theft, or diversion of special nuclear material.
- Allow 10 minutes for discussion.
- Use the answer key for responses and ask participants:
  - **What critical information was not included in the sample threat analysis?**
  - Acknowledge responses. *If not provided by participants, add the theft of material for financial gain by criminals.*
  - **What were the some of the significant points of the case study?**
  - Acknowledge responses. *If not provided by participants, add the following:*
    - *November 9, 2007, four armed gunmen entered the Emergency Control Room of the facility; they breached an electrified fence, circumvented closed-circuit television*

units (security cameras), and traveled undetected approximately 1.2 kilometers to reach the Emergency Control Room.
    - *Once inside, an employee was able to call the Security Control Center before the adversaries confronted and injured him; the gunmen assaulted and held captive a second employee.*
    - *A second group of gunmen attempted to cut through a perimeter fence; they exchanged gunfire with a security officer and retreated, failing to enter the facility.*
    - *Both groups retreated and departed from the facility; there is debate over the asset the gunmen sought. However, security experts believe the attackers were after weapons-grade uranium.*
- **What were some of the security countermeasure failures?**
- Acknowledge responses. *If not provided by participants, add:*
    - *Failure to have a secondary Emergency Control Room that monitored activity in the primary Emergency Control Room*
    - *The length of time the security force took (24 minutes) to travel the one kilometer to respond to the Emergency Control Room call for assistance*
    - *The failure of the two closed-circuit television operators to observe the attackers*
- Ask participants whether they have any questions about anything covered this far.

Topic: Potential Adversary Threats	**80 Minutes**

Enabling Learning Objective:
- Explain the types of potential adversary threats.

Slide 10 Potential Adversary Threats

- This section will cover:
    - Adversary categories
    - Potential actions of an adversary
    - Adversary motivations
    - Adversary tactics
    - Adversary capabilities and limitations

Graphic Description: No Graphic

- Define **adversary:** an individual, group, organization, or government that conducts activities, or has the intention and capability to conduct activities, detrimental to a government or facility.
- State the information participants must gather about potential threats as shown on the slide.
- Explain that the next section will present the type of information to collect about potential threats.

Slide 11 Adversary Categories (1 of 2)

- Insiders — individuals with authorized access

▪ Outsiders — individuals without authorized access ▪ Insider working together with an outsider
Graphic Description: No Graphic

- Tell participants that they must always consider the three adversary categories:
  - **Insiders** — individuals who are part of an organization and have authorized access to the facility and its information
  - Tell participants that the Navy Yard shooter in Washington, DC, US, on September 2013 had legitimate access and a valid pass to the Navy Yard because of his contractor work that had begun one week prior to the shooting that took the lives of twelve employees and injured four others.
  - **Outsiders** — individuals who do not have authorized access to the organization, information, or facility
  - **Insider working together with an outsider** — individuals who combine efforts with an external adversary or threat to attack an asset

Slide 12 Adversary Categories (2 of 2)
▪ Terrorists ▪ Criminals ▪ Discontented employees ▪ Activists ▪ Mentally ill persons
Graphic Description: Security guards at power plant

- Explain that the potential adversaries listed on the slide may insiders, outsiders, or both:
  - Terrorists
  - Criminals
  - Discontented employees
  - Activists
  - Mentally ill persons
- Emphasize that security managers must also consider the kinds of limitations the adversary might face in order to realistically assess the threat; limitations will be discussed later in this module.
- Explain that participants will first study insiders, their potential threat, and a recent insider case study and then discuss the other potential adversaries.

Slide 13 Insiders

- Most dangerous adversary because of:
  - Knowledge
  - Access
  - Opportunity
  - Motivation
- Includes:
  - Employees and contractors
  - Vendors and visitors

Graphic Description: No Graphic

- Explain that insiders are part of the common groups within an organization: employees, contractors, vendors, and visitors.
- Explain that an insider can be the most dangerous adversary a critical infrastructure could be facing due to the insider's significant:
  - **Knowledge** — facility layout, strength of security force capabilities and routines, timing for possible best attack, importance of the asset, locations of weapons or sensors, and information technology systems
  - **Access** — to the facility, to internal entries, to threatened asset, to floorplans, and restricted areas; may be allowed to carry a weapon
  - **Opportunity** — can select best time of attack based on operational hours, security schedules, or employee schedules or may be able to help plan attack to maximize impact
- Explain that insiders' motivations may be greed, dissatisfaction, or coercion from adversaries or may be political or ideological motivations.
- Emphasize that because a person is an employee, never assume he or she will be free from these motivations or safe from coercion.

Slide 14 Washington Navy Yard Shooting Case Study (1 of 2) (Handout 10.2)

- Purpose: to identify the threat involved in the case study
  - Duration: 10 minutes (5-case study; 5-discussion)
  - Group composition: table groups
  - Debrief: large-group discussion

Graphic Description: No Graphic

Slide 15 Washington Navy Yard Shooting Case Study (2 of 2)

- *No Text*

Graphic Description: Surveillance video of shooter entering Navy Yard

- Refer participants to **Handout 10.2: Washington Navy Yard Shooting Case Study**.
- Introduce the case study and play video of shooter entering the Navy Yard.
- Allow 5 minutes for participants to read the case study with their assigned teams.

- Ask teams to share their answer to the following discussion question: **What kind of threat does the Washington Navy Yard Shooting incident demonstrate?**
- Acknowledge responses. *If not provided by participants, add the following: it is an example of a violent insider threat with undiagnosed mental problems.*
- Explain that following this incident, policies and procedures were implemented to ensure that:
  - Security personnel and metal detection devices are positioned at all access points.
  - Items are searched before being allowed inside the building.
- Tell participants that:
  - *Module 11: Policies and Procedures* will cover how policies and procedures can help protect critical infrastructure.
  - Mental illness will be covered later in this section.
- Tell participants they will now discuss threats by adversaries that might be insiders, outsiders, or both.

Slide 16 Terrorists
▪ Characteristics: • Are motivated by political or social objectives • Conduct hostile surveillance • Plan to kill to achieve goals • Use explosives, automatic weapons, or both • Will risk capture, injury, or death • Target critical infrastructure
Graphic Description: Blacked out profile of terrorist suspect

- Tell participants that the first category of adversaries that may be insiders, outsiders, or both are terrorists.
- Remind participants of the definition of **terrorism** quoted from the US Code in the Terrorist Trends and Tactics Handbook in *Module 7: Cybersecurity*: premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents.
- Explain the characteristics of terrorist operations as listed on the slide.
- Explain that terrorists often target critical infrastructure.
- Provide the following examples of damage by terrorists to critical infrastructure.
- Emphasize that these examples illustrate the potential threats when terrorists gain access to sensitive jobs or sites in critical infrastructure sectors.
  - In April 2013, a northern California, US, power station experienced a 52-minute sniper attack.
    - Snipers accessed an underground vault and cut telephone cables at approximately 0100.
    - During 19 minutes of methodical shooting, snipers disabled 17 giant transformers that supply power to Silicon Valley, a center of technology research in the US.
    - One minute before the first law enforcement vehicle arrived, the snipers disappeared in to the night.

    - Repairs took 27 days.
    - Information acquired during the investigation raised concerns that this was a dry run for terrorists.
- In December 2011, Greenpeace activists broke into a French nuclear site.
    - The activists draped a banner over one of the reactor containment buildings.
    - Law enforcement officials apprehended the perpetrators.
    - The vulnerability of their atomic sites damaged the reputation of and trust in the French government.
- In December 2011, terrorists attacked an oil pipeline in the Middle East.
    - The resulting damage caused massive fires.
    - Oil production dropped by 50 percent.

Slide 17 Criminals
▪ Are often motivated by financial gain ▪ Develop financial networks to fund terrorist activity ▪ Seek to avoid either capture or detection
Graphic Description: Man in handcuffs

- Tell participants that criminal adversaries may also be insiders, outsiders, or both.
- Explain that criminal adversaries are often motivated by financial gain, for example, the criminals who stole millions of US dollars' worth of switching equipment from a telecommunication provider in the United Kingdom:
    - The case revealed that an insider relayed information to the suspects about the exact locations of the equipment.
    - The criminals sold the equipment later to potential buyers who did not want to pay for new equipment.
    - Law enforcement recovered some of the stolen equipment by searching the eBay merchandising website.
    - Investigators determined that the insider's motivation was financial gain.
- Explain that while criminal activity for financial gain is not a direct terrorist action:
    - Terrorists often develop financial networks to fund terrorist activity using legal or illegal methods.
    - If more than one adversary is involved, brute force tactics are common in criminal activities.
- Tell participants that criminals avoid taking risks that will create opportunities for capture or detection.

Slide 18 Discontented Employees (1 of 2)
▪ Perceived mistreatment by boss or disagreements with co-workers ▪ May disrupt known routines with aggressive behavior, theft, sabotage, or force ▪ May risk capture or detection
Graphic Description: No Graphic

Slide 19 Discontented Employees (2 of 2)
▪ May use fear and intimidation ▪ May be an insider or an outsider with insider information
Graphic Description: No Graphic

- Explain that an employee may feel discontented for many reasons ranging from perceived mistreatment by management to a simple disagreement among co-workers and can become an extreme threat to a critical infrastructure if not identified.
- Explain that discontented employees can demonstrate terrorist activity by disrupting the normal routine at a critical infrastructure:
  - Basing disruptions on their ability and knowledge of the facility
  - Exhibiting aggressive behavior
  - Stealing equipment or critical information
  - Sabotaging equipment or computer systems
  - Making physical threats to supervisor or co-worker(s)
- Tell participants sabotage and theft will be discussed later in the module.
- Explain that discontented employees may not be concerned if their actions lead to discovery or arrest.
- Tell participants that discontented employees often use fear and intimidation as tactics to maintain their status quo and avoid disciplinary actions.
- Clarify for participants that a discontented employee may be:
  - An insider — currently employed at the facility.
  - An outsider with insider information — formerly employed at the facility and has knowledge of the facility operations, but may or may not have access to the facility.

Slide 20 Activists
▪ Oppose ecological, political, and economic programs ▪ Use violent or nonviolent tactics for direct confrontation ▪ May attempt to defeat barriers (fences and walls) ▪ May be insider or outsider
Graphic Description: No Graphic

- Explain that activists as a threat most often commit acts in opposition to certain ecological, political, and economic programs of either the government or private enterprise.
- Explain that activists may choose violent or nonviolent tactics that may disrupt regular operations at the critical infrastructure:
  - Use of violent methods include confrontations with employees, security personnel, or law enforcement officers at the facility.
    - Law enforcement may use chemicals like tear gas to disrupt, disperse, and aid in arrests of civilian protesters or mitigate their effects on critical infrastructure.
    - In some cases, activists bring gas masks to protect themselves from the effects of tear gas.

  - Use of nonviolent methods include picketing, blockades, social media postings from mobile phones, and assembly of nonviolent protestors in mass numbers.
- Tell participants that both types of tactics may involve activists attempting to evade barriers, fences, or walls.
- Explain that activists may be insiders or outsiders — or insider employees led by outside organizers.
- Provide the following example of nonviolent activist actions which occurred in 2011 at the government-owned Fujia chemical factor in Dailan, China:
  - Nearly 12,000 demonstrators marched in the city streets wearing facemasks to demand the removal of the Fujia chemical factory which produces a toxic chemical used in the production of polyester products.
  - The protestors flooded the Internet with photos and blogs of the protest faster than government censors could delete them.
  - Although the government reported that a small group of protestors threw objects at law enforcement officers, the event was considered nonviolent.
  - Officials eventually decided to close the factory in response to the protests.

Slide 21 Mentally Ill Persons (1 of 2)
▪ Known criminal with mental illness history or family history of violence ▪ Known member of a terrorist organization ▪ Appearance of being under the influence of alcohol or other drugs ▪
Graphic Description: No Graphic

Slide 22 Mentally Ill Persons (2 of 2)
▪ Undiagnosed mental illness with no outward signs ▪ May be insider or outsider
Graphic Description: No Graphic

- Explain that some mentally ill persons do have a documented history of violence, mental illness, or terrorist connections — this is helpful information when the identity of a threat is known.
- Explain that aggressive or intoxicated behavior may be a warning sign.
- Explain that this type of individual is often unpredictable and may not send any warning message to the target or asset before taking action.
- Remind participants that the shooter in the Washington Navy Yard Shooting case study did not have a diagnosed mental illness nor did he give signs of being under the influence of any substance.
- Explain that this threat type may be either an insider or outsider motivated by some perceived wrong committed by an organization or individual related to the organization.

Slide 23 Discussion Question
▪ What are some examples of damage to critical infrastructure assets caused by terrorists, criminals, discontented employees, or mentally ill persons in your country?
Graphic Description: No Graphic

- Ask participants: **What are some examples of damage to critical infrastructure assets caused by terrorists, criminals, discontented employees, or mentally ill persons in your country?**
- Acknowledge responses. *Responses will vary.*
- If participants have no experience in this area, ask the participants what they could anticipate happening in their country.
- Tell participants that the next section will cover how an adversary's potential actions might affect a critical infrastructure or its assets.

Slide 24 Potential Actions of an Adversary (1 of 2)
▪ Consider the types of crimes and terrorist attacks these various adversaries are interested in and capable of carrying out ▪ Determine which of these acts pose a credible threat to the specific site ▪ Study historical examples and trends
Graphic Description: No Graphic

- Explain that examining an adversary's potential actions includes:
  - Identifying which adversary group is likely to attack.
  - Considering the types of crimes and terrorist attacks the various adversary groups are interested in and capable of carrying out.
    - Potential actions may vary with every target and every adversary.
    - Actions are only limited by the creativity and capabilities of the adversary group.
  - Determining which of these possible crimes and terrorist attacks could pose grave concern and a credible threat to the specific critical infrastructure site.
  - Studying previous crimes and terrorist attacks against similar critical infrastructure and what type of group carried them out to determine what trends and credible adversary options those crimes and attacks might indicate.

Slide 25 Potential Actions of an Adversary (2 of 2)
▪ Sabotage — deliberate and malicious destruction or intrusion ▪ Theft — unlawful possession of property, equipment, or information ▪ Diversion of materials — unlawful movement or transfer ▪ Other violent acts — against critical people assets
Graphic Description: No Graphic

- Explain that your knowledge of how adversaries carry out the following categories of potential actions is vital to your efforts to protect critical infrastructure assets:
  - **Sabotage** — the deliberate and malicious destruction of property with the intent to cause harm to materials, equipment, facilities, and personnel or the unauthorized intrusion into computer systems with the intent to disrupt or stop operations of a facility; may also include:
    - Arson, bombing, or other methods of destruction — an obvious example is a truck bomb
    - More subtle attack methods such as vandalism and critical equipment tampering
    - Release of a computer virus into a critical control system, which may go unnoticed until the virus destroys the system
    - Release of hazardous material
    - Modification of data or proprietary information
  - **Theft** — the unlawful possession of property, equipment, information, materials, or other valuable products; may also include removal of physical items or information from a critical infrastructure.
  - **Diversion of materials** — the unlawful movement or transfer of funds, information, or equipment.
  - **Other violent actions against critical people assets** — armed assault, hostage barricade situations, hijacking, kidnapping, maiming, and assassination.
- Remind participants of the percentages for each of the terrorist tactics discussed in the Terrorist Tactics and Trends Handbook in *Module 7: Cybersecurity*:
  - Bombing: 55%
  - Armed assault: 31%
  - Hostage: 7%
  - Assassination: 6%
  - Unknown: 1%

Slide 26 Adversary Motivations
▪ Political ▪ Philosophical ▪ Social ▪ Economic ▪ Personal
Graphic Description: Law enforcement at protest

- Explain that participants should consider the motivations of the adversaries as part of the threat analysis because knowing the motivations of your adversary will enhance the design of the physical protection system, for example:
  - A group who wants to draw sympathy for their cause is less likely to kill people than a group who wants to rid the planet of people who disagree with their philosophy.
  - The security measures for the group who wants to kill as many people as possible might include stronger barriers and a larger standoff area.
  - These are expensive measures and may not be needed if the only intention of the adversary is to draw attention to their cause.

- Explain the adversary motivations listed on the slide:
  - **Political** — concerned with the structure and organization of the forms of government and communities; activities are similar to each other in practice, even if the groups are diametrically opposed on the political spectrum
  - **Philosophical** — see their objectives as infallible and non-negotiable; may follow ethnic and nationalist identities; some extreme groups may adopt an end-of-the-world viewpoint and are dangerous and unpredictable
  - **Social** — concern for policies or issues may become so contentious that they incite extremist behavior and terrorism; examples of these types of issues include:
    - HIV or AIDS
    - Ecology and the environment
    - Human rights
    - Poverty
    - Racism
  - **Economic** — concerned with financial gain; examples include theft for ransom, sale, or extortion
  - **Personal** — unique to the individual; may include desire for revenge, mental illness, or being under threat or coercion

Slide 27 Terrorist Tactics (1 of 2)
▪ Part of the threat analysis involves examining the tactics of each potential adversary ▪ Tactics may include or be a combination of: • Stealth — perform a task undetected • Force — gain access by means of the use of violence
Graphic Description: No Graphic

Slide 28 Terrorist Tactics (2 of 2)
• Force — gain access by means of the use of violence • Deceit — provide false information to gain access ▪ Help enhance the design of the physical protection system
Graphic Description: No Graphic

- Explain that in addition to adversary motivations, the threat analysis will also require participants to consider the tactics of each potential adversary or terrorist they identified.
- Remind participants that *Module 2: Introduction to Critical Infrastructure Security and Resilience* introduced these tactics.

Slide 29 Adversary Capabilities and Limitations
▪ Determine system performance requirements ▪ Define threat more clearly ▪ Include specific considerations of: • Personnel • Knowledge, skills, and experience • Types and quantity of weapons • Tools and equipment • Transportation
Graphic Description: No Graphic

- Explain that examining the adversary's specific capabilities and limitations in the threat analysis will help participants determine performance requirements for the physical protection system — the vulnerability of the physical protection system depends on the overall capabilities and limitations of the adversary or terrorist.
- Explain that by identifying the types of capabilities and limitations possessed by the adversary:
  - Participants will be able to realistically assess the data and provide a clearer definition of the threat that exists.
  - Based on the type of facility, participants can determine in advance the kind of planning required for the adversary to achieve the objective.
- Explain the use of limitations with the following example:
  - The threat statement will be based on intelligence or informational resources.
  - If the results of the threat statement indicate that access to explosive material is extremely difficult because of strict border surveillance and no indication of manufacturing explosives in country, the terrorists will be limited on the type of attack they will try to carry out.
  - Limitations are often based on tactics, access to equipment, or successful past tactical actions.
- Explain that participants should consider the adversary's capabilities and limitations in the following areas:
  - **Personnel** — number and insider or outsider classification of the adversaries
  - **Knowledge, skills, and experience** — including:
    - Technical knowledge
    - Training and experience in the operations required to defeat the physical protection system
    - Work capacity and ability to carry equipment
  - **Types and quantity of weapons:**
    - Explosives and illegal weapons
    - Availability and accessibility
  - **Tools and equipment:**
    - Availability and necessity to accomplished identified tasks
    - Hand tools or power generators
  - **Transportation** — types of vehicles needed and their accessibility:

  - Specialty vehicles such as four-wheel drive and armored transports, special purpose trucks
  - All-terrain vehicles, motorcycles, mopeds, and bicycles
  - Aircraft and parachutes
  - Watercraft
- Tell participants that the adversary's knowledge base is dependent on the amount of information known about the facility, for example:
  - A single theft target may require a team of highly knowledgeable and trained adversaries to accomplish the goal.
  - A desire to commit an act of sabotage may only require the action of a single individual.
- Ask participants whether they have any questions about the kinds of information they need to gather about potential threat or anything else covered thus far.
- Explain that now that participants know what kinds of information they need to gather about their potential threats, the next section will describe how to obtain and organize the information.

Slide 30 TeachBack Moment 

- Why is it important to analyze the threat?
- What are the different types of adversary threats?

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: **Why is it important to analyze the threat?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Gather threat data*
  - *Identify data sources*
  - *Prepare threat analysis statement*
  - *Establish physical protection system design requirements*
- Ask participants: **What are the different types of adversary threats?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Insiders — individuals with authorized access*
  - *Outsiders — individuals without authorized access*
  - *Insider working together with an outsider — individuals who combine efforts to attack an asset*
  - *Terrorists*
  - *Criminals*
  - *Discontented employees*
  - *Activists*
  - *Mentally ill persons*

Topic: Information Sources on Potential Threat — 60 Minutes

Enabling Learning Objective:
- Describe sources of information used in analyzing a threat.

Slide 31 Information Sources on Potential Threats (1 of 4)

- Threat information helps define the threat:
  - The targeted critical infrastructure asset
  - Adversary's objective

Graphic Description: Security force outside of buildings

- Explain that threat information helps define the threat as it relates to:
  - The targeted critical infrastructure asset.
  - The adversary objectives, for example theft, sabotage, and espionage.

Slide 32 Information Sources on Potential Threats (2 of 4)

- Communication with organizations that can provide information
- Sources of threat information include:
  - Law enforcement reports
  - In-country intelligence reports
  - National threat data reports

Graphic Description: No Graphic

- Explain that to collect valid threat information, participants must:
  - Contact those organizations that are primarily responsible for the collection of threat-related data.
  - Review available documentation.
- Explain that sources of a large amount of threat information could include:
  - Local or regional law enforcement agency reports
  - In-country intelligence agency reports
  - National government and private organization threat databases
  - Military and law enforcement databases
  - International security and intelligence agencies

Slide 33 Information Sources on Potential Threats (3 of 4)

  - Military and law enforcement databases
  - International intelligence agencies
- Site incident reports
- Reports of criminal or terrorist activities in the area

Graphic Description: No Graphic

Slide 34 Information Sources on Potential Threats (4 of 4)

- Contact lists for law enforcement activities
- Number and types of personnel at the facility

- Any available threat information

Graphic Description: No Graphic

- Explain that participants may review the following types of information to help identify and define capabilities and limitations of the threats in their region or nation:
  - Incident reports at the site, such as criminal reports, intelligence reports and other historical data
  - Reports of criminal or terrorist activities in the area
  - A list of contacts for law enforcement activities
  - The number of personnel at the facility and types of positions
    - Number of employees versus the number of contractors, visitors, and vendors
    - Any problems that occurred with any of these groups
    - Identification of incidents such as domestic violence, union disputes, downsizing, and other problems
  - Publically available information from sources such as the Internet, local newspapers, professional associations, and government sources, for example:
    - The US Department of State compiles lists yearly of terrorist activities that are available to the public on its website.
    - The US Department of Homeland Security website is a source of threat information for many critical infrastructures.

Slide 35 Discussion Questions

- What are other suggestions for sources of information about potential threats in your country?
- What types of similar sources of statistics on terrorist activities does your government have?

Graphic Description: No Graphic

- Ask participants:
  - **What are other suggestions for sources of information about potential threats in your country?**
  - Acknowledge responses. *Responses will vary.*
  - **What types of similar sources of statistics on terrorist activities does your government have?**
  - Acknowledge responses. *Responses will vary.*
- Tell participants that the next section will provide them with several worksheets for organizing the information they have gathered for the threat analysis.

Slide 36 Organizing Threat Information

- Formats information to help facilitate the critical decision-making process:
  - Which threats should be included in the threat spectrum?
  - What is the effectiveness of the existing physical protection system?
- Includes both types of adversaries, insider and outsider, in the threat analysis statement

Graphic Description: No Graphic

- Remind participants of the definition of **threat spectrum** from *Module 6: Critical Infrastructure Assets*: the range of potential threats to a critical infrastructure asset.
- Remind participants of **Workbook 6.2: Threat Spectrum Matrix**.
- Explain that the organization of threat information is a crucial step in threat analysis because it enables you to format the information in a way that helps to facilitate the decision making process to answer the questions:
  - Which threats should be included in the threat spectrum?
  - What is the effectiveness of the existing physical protection system?
- Explain that threat information should include both insiders and outsiders so that characteristics of both types of adversaries are part of the threat analysis statement.
- Explain that organizing information requires analytical thinking to analyze, categorize, and prioritize the information.

Slide 37 Barriers to Analytical Thinking (1 of 2) (Workbook 10.1)

- An awareness of common barriers will help:
  - Avoid critical mistakes that could negatively affect critical infrastructure protection
  - Facilitate the analytical thought process relating to the physical protection system

Graphic Description: No Graphic

Slide 38 Barriers to Analytical Thinking (2 of 2) (Workbook 10.1)

- Focus on facts not personal opinions
- Use analytical thinking processes to overcome barriers

Graphic Description: No Graphic

- Tell participants that the next section will introduce several worksheets that provide a framework for compiling the volumes of information about potential threats participants will need to prepare their threat analysis statement.
- Explain that before participants begin to complete the worksheets, they should be aware of the common barriers to a reasonable, systemic analysis of their critical infrastructure security — this awareness may:
  - Help participants avoid critical mistakes that could negatively affect the protection of critical infrastructure assets.
  - Facilitate the analytical thought process as participants consider the physical protection system for their critical infrastructure.
- Emphasize that participants should use only facts when organizing and analyzing threat information — participants should not allow their personal opinions to influence the organizational process.
- Refer participants **Workbook 10.1: Analytical Thinking**.
- Allow participants about 5 minutes to read *Table 1: Analytical Thinking Barriers* in the addendum.

- Use the addendum to discuss the following barriers to analytical thinking:
  - Inability to control information
  - Assumptions and biases
  - Deception
  - Pattern recognition

Slide 39 Discussion Questions
▪ In your experience, which types of barriers to analytical thinking have you encountered? ▪ What actions could you take to prevent or avoid these barriers?
Graphic Description: No Graphic

- Ask participants:
  - **In your experience, which types of barriers to analytical thinking have you encountered?**
  - Acknowledge responses. *Responses will vary.*
  - **What actions could you take to prevent or avoid these barriers?**
  - Acknowledge responses. *Responses will vary.*

Slide 40 Alternative Outcome Thinking Techniques (Workbook 10.1) 
▪ Advocating the opposite view ▪ Team A or Team B analysis ▪ Other team analysis ▪ "What if?" analysis ▪ High consequence and low probability analysis ▪ Outside-in-thinking ▪ Gaming and simulation
Graphic Description: No Graphic

- Tell participants there are techniques to help promote an alternative outcome.
- Allow participants about 5 minutes to read *Table 2: Alternative Outcome Thinking Techniques* in the addendum.
- Use the addendum to discuss the advantages and disadvantages of the following processes to help think analytically:
  - Advocating the opposite view
  - Team A or Team B analysis
  - Other team analysis
  - "What if?" analysis
  - High consequence and low probability analysis
  - Outside-in-thinking
  - Gaming and simulation
- Tell participants that in the next section, they will have the opportunity to practice organizing and analyzing gathered threat information using a series of worksheets completed as they collect information.

Slide 41 Insider Threat Information Worksheet
▪ Begin threat analysis by considering unique potential insider threats posed by insiders at the critical infrastructure facility ▪ Rate and organize the insider threat information on a worksheet
Graphic Description: Man conducting assessment

- Explain that the threat analysis process should begin with a close consideration of the unique potential threats of an insider.
- Tell participants that they should organize this information by rating the insiders' knowledge, access, and opportunity to facilitate an attack on a worksheet.
- Explain that in the next activity, participants will discuss an insider threat information worksheet example.

Slide 42 Insider Threat Information Worksheet Activity (Workbook 10.2) 
▪ Purpose: to help organize gathered information about insider threats • Duration: 15 minutes (5-reading; 10-discussion) • Group composition: table groups • Debrief: large-group discussion
Graphic Description: No Graphic

- Refer participants to **Workbook 10.2: Insider Threat Worksheet Activity, Part 1: Insider Threat Information Worksheet Example**.
- Define **access:** the ability to gain entrance to the asset.
- Allow groups 5 minutes to read the information Part 1 of the addendum.
- Explain the sections of the sample insider threat worksheet in *Table 1: Sample Insider Threat Information Worksheet.*
- Remind participants that although this example uses the scale of high, medium, and low, they may find a scale with more categories useful — such as very high, high, medium, low, or very low.
- Refer participants to **Workbook 10.2: Insider Threat Worksheet Activity, Part 2: Completed Insider Threat Information Worksheet.**
- Allow 10 minutes for the large-group discussion.
- Discuss the logic for possible high, medium, or low ratings for each threat category as a group to complete *Table 2: Completed Example Insider Threat Information Worksheet* in **Workbook 10.2: Insider Threat Worksheet Activity Answer Key**.
- Ask participants whether they have any other category to add to the bottom row of the matrix and discuss the logic for rating those categories.

Slide 43 Outsider Threat Information Worksheet (Workbook 10.3)

- Organized by an assessment of potential threat:
  - Actions
  - Motivations
  - Tactics
  - Capabilities

Graphic Description: No Graphic

- Explain that participants should follow the insider threat analysis with a careful analysis of any gathered outsider threat information.
- Tell participants that they should organize this information on a worksheet by assessing outsiders' potential threats in the following categories:
  - Actions
  - Motivations
  - Tactics
  - Capabilities
- Refer participants to **Workbook 10.3: Outsider Threat Worksheet Activity, Part 1: Outsider Threat Information Worksheet Example**.
- Explain the organization of the outsider threat information worksheet in *Table 1: Sample Outsider Threat Information Worksheet*:
  - Write the threats across the top of the worksheet.
  - Write potential actions, motivations, tactics, and capabilities in the **Threat Type** column.
  - Rate the potential actions, motivations, tactics, and capabilities of the adversaries for each threat in the appropriate **Threat 1** or **Threat 2** columns.
- Explain that in the next activity, participants will discuss an outsider threat information worksheet example.

Slide 44 Outsider Threat Worksheet Activity (Workbook 10.3)

- Purpose: to help organize gathered information about outsider threats
  - Duration: 15 minutes (5-reading; 10-debrief)
  - Group composition: table groups
  - Debrief: large-group discussion

Graphic Description: No Graphic

- Refer participants to **Workbook 10.3: Outsider Threat Worksheet Activity, Part 2: Completed Outsider Threat Information Worksheet**,
- Explain the completed example in the column for **Threat 1 (Example)** in *Table 2: Completed Outsider Threat Information Worksheet:*
  - Threat type
  - Potential action
  - Motivations
  - Tactics
  - Capabilities

- Remind participants that, although this example uses the scale of high, medium, and low, they may find a scale with more categories useful — such as very high, high, medium, low, or very low.
- Allow 5 minutes for the discussion of **Threat 1 (Example)** column of *Table 2*.
- Tell participants they will now have the opportunity to complete the information for the **Threat 2** column in *Table 2* of the worksheet.
- Allow 10 minutes for the large-group discussion to complete the **Threat 2** column.
- Discuss the logic for all the entries for each category as a group to complete *Table 2: Completed Outsider Threat Information Worksheet* in **Addendum 10.5: Outsider Threat Worksheet Activity Answer Key**.
- Explain that participant responses may vary, depending on the rationale identified by each group.
- Ask participants whether they have any additional information to add to the **Other** category in each section of the worksheet and discuss the logic for those categories.

Slide 45 Estimating Likelihood of Attack (1 of 2) (Addendum 10.4)

- Determine information about each terrorist:
  - Threat type
  - Capability
  - History and intent
  - Target appeal (attractiveness)

Graphic Description: No Graphic

- Refer participants to **Workbook 10.4: Estimating Likelihood of Attack Activity.**
- Explain that once participants have completed their insider and outsider threat information worksheets, they will then estimate the likelihood of an attack by those threats.
- Use the addendum to explain each of the sections in the **Estimating Likelihood of Attack Worksheet**.
- Explain that participants must determine the following categories of information about each terrorist from the information they collected:
  - Threat type
  - Capability
  - History and intent
  - Target appeal (attractiveness)

Slide 46 Estimating Likelihood of Attack (2 of 2) (Workbook 10.4)

- Rating scale:
  - Very low
  - Low
  - Medium
  - High
  - Very high
- Numerical scale to rate threat type: 1–10, with 10 being highest

Graphic Description: No Graphic

- Refer participants to *Table 1: Estimating Likelihood of Attack Worksheet* in **Workbook 10.4: Estimating Likelihood of Attack Activity, Part 1.**
- Use the addendum to explain the rating scale range of very low to very high for the likelihood of attack.
- Explain that participants will also rate each type of threat with a numeric rating scale from 1 to 10, with a rating of 10 being the highest likelihood of attack for a particular threat.
- Tell participants they will use both of these scales to estimate the likelihood of an attack by various threats during the next activity.

Slide 47 Estimating Likelihood of Attack Worksheet Activity (Workbook 10.4)

- Purpose: to provide an example to help estimate the likelihood of attack of an identified threat
  - Duration: 25 minutes (20-activity; 5-debrief)
  - Group composition: table groups
  - Debrief: large-group discussion

Graphic Description: No Graphic

- Refer participants to **Addendum 10.6: Estimating Likelihood of Attack Activity, Part 2: Activity Directions.**
- Explain that once participants have completed their threat information worksheets, they will then estimate the likelihood of an attack.
- Discuss the directions for Part 2 of the activity
- Tell participants they will use the information given in the Air Force Base Scenario in the addendum to complete *Table 1: Estimating Likelihood of Attack Worksheet*.
- Allow 20 minutes to complete the worksheet.
- Ask each table group for their scores for Table 1.
- Briefly discuss any differences in the scores.

Slide 48 Steps to Prepare a Threat Analysis Statement (Workbook 10.5)

1. Compare the likelihood of attack for all threat types
2. Identify the most likely threat type
3. Prepare threat analysis statement

Graphic Description: No Graphic

- Refer participants to **Workbook 10.5: Preparing a Threat Analysis Statement Activity, Part 1: Threat Analysis Statement Preparation Steps**.
- Use the addendum to explain the threat analysis preparation steps:
  1. Compare the likelihood of attack for all threat types — determines the probability that an attack will occur.

2. Identify the most likely threat type — helps determine which threat can be expected, for example bombing versus direct assault.
3. Prepare threat analysis statement — provides a summary statement of the analysis results.

- Refer participants back to the sample threat analysis statements in **Addendum 10.1: Sample Threat Analysis Statement Case Study**.

Slide 49 Preparing a Threat Analysis Statement Activity (Workbook 10.5) 

- Purpose: to prepare a threat analysis statement using a given scenario
  - Duration: 15 minutes (10-activity; 5-debrief)
  - Group composition: table groups
  - Debrief: large-group discussion

Graphic Description: No Graphic

- Refer participants to **Workbook 10.5: Preparing a Threat Analysis Statement Activity, Parts 2 and 3**.
- Tell participants they will also be using **Workbook 10.4: Estimating Likelihood of Attack Activity** as a resource for this activity.
- Explain that participants will use **Part 2: Air Force Base Scenario Information** to determine the information that should be written into the threat analysis statement.
- Tell participants they will then develop and write the threat analysis statement in the space provided in **Part 3: Air Force Base Threat Analysis Statement**.
- Explain that participants may add any other known elements to the statement, for example, if intelligence reports indicated the type of weapons accessible to this threat, then participants could add that information to the statement.
- Allow 10 minutes for participants to complete the threat analysis statement activity.
- Refer to **Workbook 10.5: Preparing a Threat Analysis Statement Activity Answer Key, Part 3** during the debrief.
- Ask two of the teams to read their statements and provide feedback.
- Ask the other teams to add anything else they think should be included.
- Discuss how the threat analysis statement incorporates the elements of the worksheet.
- Be prepared to discuss a possible threat analysis statement for the host facility.
- Ask participants whether they have questions about anything covered so far.

Slide 50 Community Engagement and Human Rights Discussion 

- Why is it important to engage the community in determining the types of threats that may exist?

Graphic Description: No Graphic

- Lead a brief discussion related to human rights and community engagement. For example, ask participants: **Why is it important to engage the community in determining the types of threats that may exist?**
- Acknowledge response. *If not provided by participants, add the following:*

  - *If there are community-based information programs, community input may help identify possible threats or subjects*
  - *The community can be the eyes and ears of law enforcement*
- Tell participants they 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 3 — National Ministries Building	**60 Minutes**

Enabling Learning Objective:
- Develop a threat analysis statement for a given critical infrastructure.

Slide 51 Threaded Exercise Part 3 — National Ministries Building

- Purpose: to prepare a threat analysis statement
  - Duration: 60 minutes (45-exercise; 15-debrief)
  - Group composition: table groups
  - Debrief: presentation and discussion

Graphic Description: No Graphic

Slide 52 National Ministries Building Complex Map

- *No Text*

Graphic Description: Map of National Ministries Building and surrounding buildings

- Refer to facilitator **Threaded Exercise Workbook Part 3 — National Ministries Building Answer Key** for answers to Part 3 of the National Ministries Building Threaded Exercise.
- Refer participants to **Threaded Exercise Workbook Part 3 — 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 2: Introduction to Critical Infrastructure Security and Resilience*.
- Assign either the insider threat or the outsider threat to each group.
- Assign an interpreter to each team as needed.
- Discuss the introduction and directions for **Threaded Exercise Workbook Part 3 — National Ministries Building, 3.1 Prepare the Threat Analysis**.
- Tell teams to use the information in the following addendums as resources to help them complete their work in the threaded exercise:
  - **Addendum 10.4: Insider Adversary Threat**
  - **Addendum 10.5: Outsider Adversary Threat**
  - **Addendum 10.6: Estimating Likelihood of Attack**
  - **Addendum 10.7: Preparing a Threat Analysis Statement Activity**
- Tell participants to read the information provided in **3.2 National Ministries Building Data Collection** and complete the worksheets in the following tables:

- *Table 4: Insider Threat Information Worksheet*
- *Table 5: Outsider Threat Information Worksheet*
- *Table 6: Estimating Likelihood of Attack (L_A) Worksheet (1)*
- *Table 7: Estimating Likelihood of Attack (L_A) Worksheet (2)*

- Explain that once the teams have completed the worksheets, they should prepare the threat analysis statements in **3.3 Threat Analysis Statements** for the identified threats using the space provided in their workbook.
- Allow the groups 45 minutes to complete the worksheets and write the threat analysis statements.
- Remind participants that the process of writing a threat analysis statement is an art, not a science.
  - Informed reviewers analyze the information they have gathered and make judgments in order to categorize and prioritize the information.
  - There are no correct and incorrect answers.
  - Therefore, teams should base their analysis statement on the information received.
  - Teams must ensure they are analyzing facts and not making decisions based on opinion.
  - The data has to support the team's conclusion.
- Explain that although the team members may not agree, the dialog is important in understanding the threats against the National Ministries Building.
- Tell teams they should be prepared to discuss their responses and rationale for each rating.
- Allow 15 minutes for the presentations and discussion.
- Facilitators should walk around the room as participants work to ensure that any questions the participants have can be answered.
- Refer to **Threaded Exercise Workbook Part 3 — National Ministries Building Answer Key** for discussion and debrief.
- Once participants complete the exercise, call on individual teams to present their answers to the class.
- Throughout the exercise, ask questions and encourage discussion.

Topic: Module Summary	**10 Minutes**

Slide 53 Module Summary
▪ Purpose of the threat analysis ▪ Potential adversary threats ▪ Information sources on potential threat
Graphic Description: No Graphic

- Summarize the module by reviewing the following main points:
  - **Purpose of the threat analysis**
    - Gather threat data
    - Identify data sources
    - Prepare threat analysis statement

    - Establish physical protection system design requirements
  - **Potential adversary threats**
    - Categories
    - Potential actions
    - Motivations
    - Tactics
    - Capabilities and limitations
  - **Information sources on potential threat**
    - Threat information helps define the targeted critical infrastructure asset and adversary's objective
    - Sources of threat information
    - Common barriers to analytical thinking
    - Develop insider and outsider threat information worksheets
    - Estimate likelihood of attack
    - Prepare a threat analysis statement using three steps
- Ask whether there are any questions about the contents of this module.
- Explain that *Module 11: Policies and Procedures* will describe the types of policies and procedures needed for the protection of critical infrastructure.