MODULE 15: OPERATIONAL RESILIENCE

Day: 7 **Time:** 3.0 Hours **Level of Understanding:** Application

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

Module Equipment/Facilities:
- Standard Classroom Setup
- Handout 15.1: Gap Analysis Process Scenario Activity Answer Key
- Threaded Exercise — National Ministries Building, Part 8: Operational Resilience Plan Answer Key
- National Ministries Complex Map

Participant Materials/Handouts:
- Handout 15.1: Gap Analysis Process Scenario Activity
- Threaded Exercise Workbook Part 8 — National Ministries Building

Terminal Learning Objective

By the end of this module, you will be able to describe how to apply operational resilience strategies for your country after a terrorist attack, natural disaster, or other threat.

Introduction

Recall that in *Module 14: Security Inspection and Validation*, the results of the security inspection and validation may reveal deficiencies or potential gaps that exist in the current physical protection system. The recommended security inspection and validation program provided you with a process for identifying the requirements of an effective physical protection system in the areas of policies and procedures, security force personnel, and security technologies.

Your national security and standard of living depend on the reliable functioning of your critical infrastructure that include many types of assets, networks, and systems such as food, water, energy, communications, transportation, and banking. The destruction of your critical infrastructure could immobilize your national security, economy, and public health and safety. Collectively, your infrastructure sectors provide the foundation of your economy and society.

The risks you face as a nation are complex. They include human-caused threats that range from terrorist attacks to cyberthreats and natural disasters that range from power outages to mass destruction caused by hurricanes, earthquakes, or floods. The complex connections

and physical characteristics of your infrastructure make it essential that you identify and reduce vulnerabilities. Ensuring the continued operation of your infrastructure requires a plan to achieve resilience so that regardless of the threats electricity flows, communications remain active, and transportation continues to operate.

In this module, you will examine the need to maintain critical operations and functions in a crisis; prepare for, respond to, and manage a crisis or disruption as it occurs; and resume normal operations quickly and efficiently. Security and resilience complement each other and are both necessary elements of a comprehensive risk management strategy. Protecting and ensuring the resilience of your critical infrastructure is a shared responsibility that involves all levels of government in partnership with owners and operators.

At the end of the module, you will use the knowledge you have gained to develop a resilience plan and provide a recommendation for a security upgrade to the National Ministries Building.

Module Topics

An outline of key topics and an approximate time plan are shown below.

Topic	Enabling Learning Objectives	Approximate Time
Module Introduction	▪ Not Applicable	5 minutes
Critical Infrastructure Resilience	▪ Define resilience, collaboration, and protection as they relate to critical infrastructure resilience. ▪ Discuss critical infrastructure resilience as it applies in your country.	15 minutes
Critical Infrastructure Security and Resilience Policy Example	▪ Describe an example of a policy directive relating to critical infrastructure resilience.	30 minutes
Planning for Resilience Threaded Exercise Part 8 — National Ministries Building	▪ Explain how to develop an operational resilience plan.	120 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
Collaboration	The process of working together to achieve shared goals
Gap analysis process	The steps that security managers use to compare the **actual** performance of an existing physical protection system with its **potential** performance
Protection	The capabilities necessary to secure the homeland against acts of terrorism and human or natural disasters

Topic: Module Introduction — 5 Minutes

Slide 1 Operational Resilience

- Title Slide

Graphic Description: US Flag and Seal

Module Preparation

- **Timing and Methods:** Use the suggested time plan at the beginning of the module. As with all modules in this course, read all the content (Facilitator Guide and PowerPoint slides) and familiarize yourself with each facilitator note before class.
- Be thoroughly prepared for exercises, discussions, or other activities required for the module. Follow all facilitator notes. Use a combination of lecture, large-group discussion, small-group activities, and TeachBack moments.

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 the 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 describe how to apply operational resilience strategies for your country after a terrorist attack, natural disaster, or other threat

Graphic Description: No Graphic

- Briefly discuss the terminal learning objective.
- Highlight the key topics to be presented:
  - Critical Infrastructure Resilience
  - Critical Infrastructure Security and Resilience Policy Example
  - Planning for Resilience
- Ask participants whether they have any questions about anything covered thus far.

Slide 3 Course Map Diagram

- *No Text*

Graphic Description: Physical protection system diagram with Develop Operational Resilience box highlighted in yellow

- Recall from the previous modules that there are four phases in the vulnerability analysis process.
  - Modules 2, 5, and 6 introduced the steps included in *Phase 1: Identify Critical Infrastructure, Assess Critical Infrastructure Components,* and *Identify Critical Infrastructure Assets*.
  - Modules 7–10 discussed *Phase 2: Analyze the Threat*, which included a discussion of cybersecurity, surveillance detection, explosives and critical infrastructure, and how to create a Threat Analysis Statement.
  - Modules 11–14 introduced *Phase 3: Identify Security Countermeasures*. Three primary countermeasures were discussed: policies and procedures, security force, and security technology. *Module 14: Security Inspection and Validation* provided information on how to evaluate the existing security countermeasures of a physical protection system.
- In this module, the physical protection system diagram illustrates *Phase 4: Develop Operational Resilience* as the last step of the vulnerability analysis process.
- Tell participants the next section will present various terms related to critical infrastructure resilience.

Topic: Critical Infrastructure Resilience — 15 Minutes

Enabling Learning Objectives:
- Define resilience, collaboration, and protection as they relate to critical infrastructure resilience.
- Discuss critical infrastructure resilience as it applies in your country.

Slide 4 Terms Related to Critical Infrastructure Resilience

- Resilience — to prepare and adapt, withstand and recover rapidly
- Collaboration — to work together to achieve shared goals
- Protection — the capabilities necessary to secure the homeland

Graphic Description: No Graphic

- Remind participants of the definition for **resilience** in *Module 2: Introduction to Critical Infrastructure Security and Resilience*: the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions such as deliberate attacks, accidents, or naturally occurring threats or incidents.
- Define:
  - **Collaboration:** the process of working together to achieve shared goals.
  - **Protection:** the capabilities necessary to secure the homeland against acts of terrorism and human or natural disasters.

Slide 5 Resilience in Your Country (1 of 2)
▪ What strategies does your country currently have for resilience? ▪ What types of capabilities does your country have to protect against threats and natural disasters?
Graphic Description: No Graphic

Slide 6 Resilience in Your Country (2 of 2)
▪ What type of preparations for resilience has your country made? ▪ Based on your country's past experience, how long has it taken to return to operational status?
Graphic Description: No Graphic

- Lead a large-group discussion about resilience in the participants' country.
- Ask participants: **What strategies does your country currently have for resilience?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Developing resilience plans*
  - *Developing partnerships with the business sector to address cross-functional collaboration*
- Ask participants: **What types of capabilities does your country have to protect against threats and natural disasters?**
- Acknowledge responses. *Responses will vary.*
- Ask participants: **What type of preparations for resilience has your country made?**
- Acknowledge responses. *Responses will vary.*
- Ask participants: **Based on your country's past experience, how long has it taken to return to operational status?**
- Acknowledge responses. *Responses will vary.*
- Tell participants that the next section will cover policy directives that relate to critical infrastructure resilience.

Topic: Critical Infrastructure Security and Resilience Policy Example — 30 Minutes

Enabling Learning Objective:

- Describe an example of a policy directive relating to critical infrastructure resilience.

Slide 7 Critical Infrastructure Security and Resilience Policy Example
▪ High-level national directive to serve as a template for other sectors; may include: • Introduction • Policies • Roles and responsibilities • Strategic imperatives • Innovations and research and development • Actions to implement the directive

Graphic Description: No Graphic

- Tell participants that critical infrastructure security and resilience depends on national policies designed to unify the efforts to strengthen and maintain secure, functioning, prepared, and adaptable critical infrastructure.
- Explain that the policy described in this topic is a policy directive from a US president giving direction to Congress on what policies, procedures, and actions must take place for the United States to have a national security and resilience policy generated at the highest level that provides a template for the sixteen categories.
- Explain that while the example directive has the sections listed below, your government may decide that other sections are needed or that some of these are unnecessary in your country:
  - Introduction
  - Policies
  - Roles and responsibilities
  - Strategic imperatives
  - Innovations and research and development
  - Actions to implement the directive

Slide 8 Critical Infrastructure Security Introduction (1 of 3)

- Requires coordinated efforts
- Includes both physical space, cyberspace, and multinational ownership
- Requires managing risk and determining effective strategies for resilience
- Helps rapid recovery

Graphic Description: No Graphic

- Explain that the coordinated efforts necessary to maintain the security of a nation's critical infrastructure — including assets, networks, and systems — is vital to public confidence and the nation's safety, prosperity and well-being.
- Tell participants that the diverse and complex nature of critical infrastructure includes both physical space and cyberspace and may include multinational ownership.
- Explain that critical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient.
- Emphasize that critical infrastructure must be secure and able to withstand and rapidly recover from all hazards.

Slide 9 Critical Infrastructure Security Introduction (2 of 3)

- Requires security systems integration across:
  - Prevention
  - Preparedness
  - Response
  - Recovery

Graphic Description: No Graphic

- Explain that achieving this security and strength will require integration with critical incident management security systems across:
  - Prevention
  - Preparedness
  - Response
  - Recovery
- Refer participants back to *Module 11: Policies and Procedures* for definitions of each phase.

Slide 10 Critical Infrastructure Security Introduction (3 of 3)

- Requires all stakeholders to share policies and action
- Compels national governments to strengthen internal security and resilience

Graphic Description: No Graphic

- Explain that policies and action to achieve this goal must be shared between of all stakeholders involved, including all levels of governments or agencies and public and private owners and operators of critical infrastructure.
- Explain that the national government also has a responsibility to strengthen the security and resilience of its own critical infrastructure:
  - For the continuity of national essential functions.
  - To collaborate effectively with and add value to the security and resilience efforts of critical infrastructure owners and operators.

Slide 11 Critical Infrastructure Resilience Policies (1 of 2)

- Governments and stakeholders work to:
  - Take proactive steps to manage risk
  - Consider all hazards to security, economy, health, and safety
  - Integrate policies to reflect interdependencies
  - Identify critical energy and communication systems
  - Protect all information in compliance with law

Graphic Description: No Graphic

- Explain that policies help governments and other stakeholders work together to:
  - Take proactive steps to manage risk and strengthen the security and resilience.
  - Consider all hazards that could have a devastating effect on:
    - National security.
    - Economic stability.
    - Public health and safety.
    - Any combination of these.
  - Address integrated security and resilience to reflect the infrastructure's interconnectedness and interdependency.

- Identify energy and communications systems as especially critical due to the enabling functions they provide across all sixteen categories.
- Protect all information associated with carrying out resilience policies in compliance with applicable legal authorities and policies.

Slide 12 Critical Infrastructure Resilience Policies (2 of 2)
▪ Reduce vulnerabilities ▪ Minimize consequences ▪ Identify and disrupt threats ▪ Hasten response and recovery efforts
Graphic Description: No Graphic

- Explain that well-written resilience policies for critical infrastructure should attempt to:
  - Reduce vulnerabilities.
  - Minimize consequences.
  - Identify and disrupt threats.
  - Hasten response and recovery efforts.

Slide 13 Roles and Responsibilities (1 of 2)
▪ Minister or secretary of national security and resilience organization: • Provide high-level strategic guidance • Promote and coordinate national unity • Evaluate national capabilities and analyze threats • Identify security and resilience functions • Develop a national plan and report effectiveness
Graphic Description: No Graphic

- Explain the primary responsibilities of a minister or secretary as leader of a national security and resilience organization:
  - **Provide strategic guidance** from the highest level.
  - **Promote and coordinate** the overall effort of a national organization to promote the security and resilience of the country's critical infrastructure.
  - **Evaluate national capabilities**, opportunities, and challenges in protecting critical infrastructure.
  - **Analyze threats** to, vulnerabilities of, and potential consequences from all human threats and natural disasters on critical infrastructure.
  - **Identify security and resilience functions** that are necessary for effective public-private engagement with all critical infrastructure sectors.
  - **Develop a national plan**, in coordination with primary stakeholders and other critical infrastructure partners.
    - **Integrate and coordinate** national cross-sector security and resilience activities.
    - **Identify and analyze** crucial interdependencies among critical infrastructure sectors.

- **Report effectiveness** of the national efforts to strengthen the national security and resilience position for critical infrastructure.

Slide 14 Roles and Responsibilities (2 of 2)
▪ Sector-specific agencies: • Unique characteristics, operating models, and risk profiles • Institutional knowledge and specialized expertise • Knowledge of specific recovery and resilience needs
Graphic Description: No Graphic

- Remind participants of the sixteen critical infrastructure categories discussed earlier in this course:
  - Each category is a sector that has unique characteristics, operating models, and risk profiles.
  - Each category would benefit from establishing a sector-specific agency having institutional knowledge and specialized expertise about that sector.
  - Each specific agency would know what the critical infrastructure needs in the event of a critical incident and how to conduct recovery and resilience efforts.

Slide 15 Roles and Responsibilities of Other Stakeholders
▪ Finance and contracts division ▪ Human resources division ▪ Information technology division ▪ Legal division ▪ Operational area specialists ▪ Security operations team
Graphic Description: Stakeholder team at meeting at conference table

- Explain that the gap analysis process and ensuing discussions on how to mitigate risk are the primary responsibility of security professionals.
- Tell participants that the decisions concerning security issue(s) will require a collaborative effort with several of the different stakeholder groups across the sixteen different categories:
  - **Finance and contracts division** — assists in developing funding sources and developing contractual agreements that specifically define contract requirements.
  - **Human resources division** — provides feedback to labor costs and the ability to hire additional personnel with specific job competencies; also provides additional input for training issues for personnel prior to deployment and during job performance, as needed.
  - **Information technology division** — assists in ensuring that the organization can integrate any technology solutions into existing information technology systems.
  - **Legal division** — identifies legal, policy, and contractual controls for the organization, which include corporate liability and other business issues.

- **Operational area specialists** — defines the function and requirements to maintain daily operations.
- **Security operations team** — selects control solutions based on recommendations from the security inspection and validation team.

Slide 16 Three Strategic Imperatives (1 of 3)

1. Refine and clarify functional relationships across the government to advance the national unity of effort to strengthen critical infrastructure security and resilience:
   - Guided by a national plan
   - Informed by expertise, experience, capabilities, and responsibilities of all stakeholders

Graphic Description: No Graphic

- Explain that three strategic imperatives will help accomplish strengthening of critical infrastructure security and resilience.
- Explain that an effective national effort to strengthen critical infrastructure security and resilience must be:
  - Guided by a national plan that identifies roles and responsibilities.
  - Informed by the expertise, experience, capabilities, and responsibilities of all stakeholders involved, including all levels of government or organizations and public and private owners and operators of critical infrastructure.
- Explain that governments may consider establishing two national critical infrastructure centers — one for physical infrastructure, one for cyberinfrastructure.
- Explain that these centers will be integrated and serve as focal points for critical infrastructure partners to obtain situational awareness and integrated, actionable information to protect the physical and cyber aspects of critical infrastructure.
- Explain that the vulnerabilities between these two aspects are closely linked and will be discussed in the third imperative.
- Tell participants that these national centers should not hinder the ability of government leaders and law enforcement agencies to carry out or perform their responsibilities for national defense, criminal, counterintelligence, counterterrorism, or investigative activities.

Slide 17 Three Strategic Imperatives (2 of 3)

2. Enable efficient information exchange by identifying baseline data and systems requirements for the government:
   - Timely exchange
   - Situational awareness capability
   - System requirements
   - Respect of privacy and civil liberties

Graphic Description: No Graphic

- Explain that a secure, functioning, and resilient critical infrastructure requires the efficient exchange of information, including intelligence, between all levels of government and critical infrastructure owners and operators that includes:
  - Timely exchange of threat and vulnerability information.
  - Information that allows for the development of a situational awareness capability during incidents.
  - Identification of requirements for:
    - Data and information formats and accessibility.
    - System interoperability.
    - Redundant systems and alternate capabilities should there be a disruption in the primary systems.
- Explain that greater information sharing within the government and with the private sector can and must be done while respecting privacy and civil liberties:
  - Ensure that all existing privacy principles, policies, and procedures are implemented consistent with applicable law and policy.
  - Include senior agency officials for privacy in their efforts to govern and oversee information sharing properly.

Slide 18 Three Strategic Imperatives (3 of 3)
3. Implement an integration and analysis function to inform planning and operational decisions regarding critical infrastructure
Graphic Description: Team in planning meeting

- Explain that this imperative builds on the first two by requesting the implementation of an integration and analysis function for critical infrastructure at the national centers that includes operational and strategic analysis on incidents, threats, and emerging risks.
- Explain that this strategic imperative:
  - Relates to the two national centers identified in the first strategic imperative.
  - Includes the capability to collate, assess, and integrate vulnerability and consequence information with threat and hazard information to:
    - Help to prioritize assets and manage risks to critical infrastructure.
    - Anticipate interdependencies and incident secondary effects that result from primary effects.
    - Recommend security and resilience measures for critical infrastructure prior to, during, and after an event or incident.
    - Support incident management and restoration efforts related to critical infrastructure.
- Explain that this integration and analysis function helps to support the government's ability to support a near real-time situational awareness capability for critical infrastructure that includes:
  - Actionable information about imminent threats.
  - Significant trends.
  - Awareness of incidents that may affect critical infrastructure.

Slide 19 Innovation and Research and Development (1 of 2)
▪ Align research and development activities ▪ Research innovations in construction and cybersecurity methods ▪ Enhance research on various scenario responses
Graphic Description: No Graphic

Slide 20 Innovation and Research and Development (2 of 2)
▪ Facilitate incentives for investments in designs ▪ Prioritize efforts to implement critical infrastructure security and resilience policies
Graphic Description: No Graphic

- Explain that national governments should support the following types of innovation and research and development to strengthen and align security and resilience across the nation and across all sector-specific agencies:
  - Align research and development activities to strengthen security and resilience of critical infrastructure.
  - Research innovations in construction and cybersecurity methods.
  - Enhance research on various scenario responses to determine effects on critical infrastructure and related effects on other sectors.
  - Facilitate incentives for investments in designs to strengthen cybersecurity and critical infrastructure security and resilience.
  - Prioritize efforts to implement critical infrastructure security and resilience policies.

Topic: Planning for Resilience — 120 Minutes

Enabling Learning Objective:
- Explain how to develop an operational resilience plan.

Slide 21 Planning for Resilience
▪ Adequacy and deficiency ▪ Timely recovery ▪ Policy applies across all sectors ▪ Each sector responsible for implementing in their area
Graphic Description: No Graphic

- Explain that determining the following will help participants plan for resilience:
  - Where resilience is adequate.
  - Where resilience is deficient.
  - How to develop a plan that will help ensure recovery and resilience occur in a timely manner.
- Explain that a national policy for critical infrastructure security and resilience is designed to be applicable across all sectors.

- Explain that each sector is responsible for implementation of the plan in their specific area of resilience.

Slide 22 Gap Analysis Process (1 of 2)
▪ The steps that security managers use to compare the **actual** performance of an existing physical protection system with its **potential** performance • Does the system design meet requirements? • Does the system meet expected outcomes?
Graphic Description: No Graphic

- Define **gap analysis:** the steps that security managers use to compare the **actual** performance of an existing physical protection system with its **potential** performance.
- Explain that a gap analysis depends on a thorough evaluation of the existing system in terms of design, operational effectiveness, and standard outcomes.
- Explain that security managers responsible for conducting a gap analysis seek to answer two basic questions:
  - Does the design of the physical protection system meet the operational requirements to function effectively for the protection of the critical infrastructure?
  - Does the physical protection system meet the expected outcomes as desired or required by the organization?

Slide 23 Gap Analysis Process (2 of 2)
▪ Step 1: Determine expected standard requirements ▪ Step 2: Assess existing performance levels ▪ Step 3: Identify gaps ▪ Step 4: Define risk management plan
Graphic Description: Diagram of four steps in the process

- Tell participants that the four steps of the gap analysis process listed on the slide will help security managers answer those two questions.

Slide 24 Step 1: Determine Expected Standard Requirements
▪ Identify the performance requirements and expectations for a specific security countermeasure
Graphic Description: Diagram of four steps in the process with Determine in bold type

- Explain that in the first step of the process, the individual conducting the gap analysis clearly identifies the performance standard requirements and expected outcomes for a specific security countermeasure.

Slide 25 Step 2: Assess Existing Performance Levels
▪ Decide how the existing performance levels will be measured
Graphic Description: Diagram of four steps in the process with Assess in bold type

- Explain that in this next step, the individual conducting the gap analysis makes a decision about how to measure the existing performance levels, such as what testing processes and metrics to use.

Slide 26 Step 3: Identify Gaps
▪ Determine what areas (risks) do not meet the pre-established performance standards or expectations
Graphic Description: Diagram of four steps in the process with Identify in bold type

- Explain that in the third step, the individual conducting the gap analysis examines the test results from Step 2 to identify areas (risks) that do not meet the pre-established performance standards or expectations outlined in Step 1.

Slide 27 Step 4: Define Risk Management Plan
▪ Determine the best countermeasures to manage the risks
Graphic Description: Diagram of four steps in the process with Define in bold type

- Explain that in the final step in the gap analysis process, the individual conducting the gap analysis makes decisions to determine how to best manage — what countermeasures will be most appropriate for — the risks identified in Step 3.

Slide 28 Gap Analysis Process Scenario Activity (Handout 15.1) 
▪ Purpose: to identify the steps of the gap analysis process in a given scenario • Duration: 40 minutes (30-activity; 10-discussion) • Group composition: table groups • Debrief: large-group discussion
Graphic Description: No Graphic

- Refer participants to **Handout 15.1: Gap Analysis Process Scenario Activity**.
- Tell participants they will continue to work with their team for this activity.
- Allow participants 30 minutes to read the scenario and then answer the discussion questions following **Option 3: Accept Responsibility and Mitigate Risk.**
- Allow 10 minutes to conduct a large-group discussion about the activity.
- Tell participants that decision makers construct the risk management plan for their organization by evaluating the three basic choices to mitigate risk:
  - Option 1: Accept the risk and do nothing
  - Option 2: Transfer the issue to another organization, such as an insurance company

  - Option 3: Accept responsibility and attempt to mitigate the risk through implementation of new or enhanced physical protection system strategies
- After teams have finished reading the scenario, ask two teams to complete the **Discussion Questions for the Fence Sensors Scenario** (the other two teams will share with the class in the next activity).
- Use the **Handout 15.1: Gap Analysis Process Scenario Activity Answer Key** to assess each team's answers.

Slide 29 Proposed Security Countermeasures

- Formulate how the proposed countermeasures will resolve the gap
- Prioritize the recommendations from security inspection and validation report:
  - Importance and vulnerability
  - Greatest risks are highest priority

Graphic Description: Officer monitoring security video monitors at a facility

- Explain that once the gap analysis is complete and the organization responsible will determine the plan to manage the risks associated with the discovered gaps, the next step is to formulate how the proposed countermeasures will resolve the gap within the physical protection system.
  - Updates to policies, procedures, and security plans
  - Deployment and redeployment of security force members
  - Additional technology measures
- Explain that prioritizing the recommendations from their organization's security inspection and validation report will assist participants as decision makers to move forward with required or desired changes.
- Remind participants that *Module 5: Critical Infrastructure Components* and *Module 6: Critical Infrastructure Assets* discussed how assessing the importance and vulnerability of your critical infrastructure will help in the prioritization of the recommendations so that those areas with the greatest risk to security are of highest priority.
- Tell participants that *Module 11: Policies and Procedures, Module 12: Security Force Operations, Module 13: Security Technology,* and *Module 14: Security Inspection and Validation* will assist them in clarifying and prioritizing their recommendations.

Slide 30 Discussion Questions

- In your experience, which type of security countermeasure is the most consistently well planned and budgeted? Why?
- In your experience, which type of security countermeasure is the least planned and budgeted? Why?

Graphic Description: No Graphic

- Ask participants the following discussion questions:
  - **In your experience, which type of security countermeasure is the most consistently well planned and budgeted? Why?**

- **In your experience, which type of security countermeasure is the least planned and budgeted? Why?**

- Acknowledge responses. *Responses will vary.*
- Facilitate disagreements amicably if there are members of different divisions from the same agency present who disagree as to why funding is provided or not provided.

Slide 31 Develop National Operational Resilience Plan (1 of 2)
▪ National security and resilience organization and minister must develop the national plan that each sector will use as a model ▪ Integrate: • Prevention • Preparedness • Response • Recovery
Graphic Description: No Graphic

- Explain that to develop an operational resilience plan that will be a national plan and template for the sixteen sectors to develop their own plans, a country's minister or secretary of the national security and resilience organization must lead and coordinate with the government and all stakeholders to develop a comprehensive operational resilience plan.
- Remind participants that the plan requires security systems integration across prevention, preparedness, response, and recovery for the sixteen sectors.
- Explain that working together, the government, resilience agencies, and stakeholders acting as advisors will collect available resilience studies and reports and then develop data as appropriate to determine recommendations for the resilience plan:
  - Assess gaps in the current conditions of existing critical facilities and lifeline systems and the capabilities of each to manage terrorist attacks, cybersecurity intrusions, natural disasters, or other threats.
  - Evaluate the effectiveness of current design and construction practices relative to each sector to be able to design in resilience.

Slide 32 Develop National Operational Resilience Plan (2 of 2)
▪ Stakeholders, government agencies, and advisory groups must coordinate together to: • Assess gaps in current conditions • Evaluate effectiveness of current practices • Develop expected outcomes and performance relative to resilience • Prepare plan of prioritized recommendations for high-level national policies, procedures, and actions
Graphic Description: No Graphic

- Develop the desired performance targets and expected outcomes in terms of usability and time required for restoration of services to meet resilience goals.

  - Prepare the plan of prioritized recommendations for high-level national policies, procedures, and actions to achieve the desired performance targets and expected outcomes — this national plan then becomes the model for each of the sixteen categories to create an operational resilience plan for its sector.
- Explain that teams will have the opportunity to select a security countermeasures they consider as the top priorities and identify and discuss the main points of a resilience plan for the National Ministries Building complex.

Slide 33 TeachBack Moment

- What are the definitions of resilience, collaboration, and protection as they relate to critical infrastructure resilience?
- What are the important elements of a critical infrastructure security and resilience directive?
- What are the necessary actions to develop an operational resilience plan?

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 definitions of resilience, collaboration, and protection as they relate to critical infrastructure resilience?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Resilience: the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions such as deliberate attacks, accidents, or naturally occurring threats or incidents.*
  - *Collaboration: the process of working together to achieve shared goals.*
  - *Protection: the capabilities necessary to secure the homeland against acts of terrorism and human or natural disasters .*
- Ask participants: **What are the important elements of a critical infrastructure security and resilience directive?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Introduction*
  - *Policies*
  - *Roles and responsibilities*
  - *Strategic imperatives*
  - *Innovations and research and development*
- Ask the participants to: **What are the necessary actions to develop an operational resilience plan?**
- Acknowledge responses. *If not provided by participants, add the following:*
  - *Assess gaps in current conditions.*
  - *Evaluate effectiveness of current practices.*
  - *Develop expected outcomes and performance relative to resilience.*
  - *Prepare plan of prioritized recommendations for high-level national policies, procedures, and actions.*

Slide 34 Threaded Exercise — National Ministries Building Part 8

- Purpose: to present four main points of an operational resilience plan statement that includes recommended security countermeasures for a given scenario
  - Duration: 70 minutes (40-preparation; 30-debrief)
  - Group composition: table groups
  - Debrief: group presentations and facilitator feedback

Graphic Description: No Graphic

Slide 35 National Ministries Building Complex Map

- *No Text*

Graphic Description: National Ministries Building complex map

- Refer participants to the security inspection and validation checklist they completed in *Module 14: Security Inspection and Validation,* **Threaded Exercise — National Ministries Building Part 7: Security Inspection and Validation**.
- Emphasize that the teams will choose only **one item** from each of the security countermeasures as the focus for of a 5-minute presentation as the outcome of the activity.
- Refer participants to **Threaded Exercise — National Ministries Building, Part 8: Operational Resilience Plan**.
- Remind participants that this process 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.
  - They must ensure they are analyzing facts and not making decisions based on opinion.
  - The data has to support the conclusion.
- Explain that although team members may not agree, the discussion of these recommendations is important in understanding the process of analyzing the security countermeasures.
- Explain that this activity is the bridge from their security inspection and validation evaluation to the resilience plan.
- Tell teams to select three questions from their Security Inspection and Validation Checklist that, if answered **No**, would pose a significant threat to the National Ministries Building.
- Tell participants to discuss these three issues and complete *Table 14: Integrating Security Inspection and Validation Results and Gap Analysis*.
- Explain that the **Results** column was completed for them as an example using information from the fence sensor scenario.
- Remind participants that the false alarm rate and nuisance alarm rate may not always be applicable. For example, if the task is to conduct random badge checks at the entrance to the critical infrastructure, then the accuracy would be less than 100% with no false alarm rate or nuisance alarm rate involved.
- Explain that the recommendations to correct these deficiencies will form the basis to outline a gap analysis, which is the first step towards a potential cost benefit analysis.

- Explain that the information needed to complete **Row 7: Collaborative Groups** may not be contained in their Security Inspection and Validation Report Recommendations and Conclusions, but they should still discuss and include which groups may be appropriate to assist in the proposed actions.
- Note: there are no pre-determined answers for this activity since teams will draw their examples from the report they generated in **Threaded Exercise Part 7 — National Ministries Building** from *Module 14: Security Inspection and Validation*.
  - **Thus, no recommendations answer key is provided to the facilitator.**
  - Use the example provided in the first column as guidance for how to complete the table.
- Complete *Table 15: Proposed Countermeasure Categories and Priorities* using the necessary information in the previous table.
- Explain that once they have categorized the recommendations according to the countermeasure category, they will check one, two, or three to prioritize them within that category. In other words, they may have a one checked for both technology and security force, if there is a recommended action for these two countermeasures.
- Tell participants that teams should prepare to discuss their responses and rationale for each final recommendation that they include in the resilience plan.
- Tell participants that after completing Tables 14 and 15, they will have the opportunity to bring the last phase of resiliency planning to the scenario of the threaded exercise.
- Explain that based on work done in this module, work with their group to complete *Table 16: Operational Resilience Plan Main Points* by developing four major points to address prevention, preparedness, response, and recovery in the plan.
- As participants work, have facilitators walk around the room to answer any questions they may have.
- Allow 40 minutes for the teams to prepare their 5-minute presentations.
- Refer to **Threaded Exercise — National Ministries Building, Part 8: Operational Resilience Plan Answer Key** for this section of the exercise.
- Once participants complete the activity, bring them together, and ask them to present their answers to the facilitators.
- Allow 30 minutes for all of the presentations and feedback.
  - Each team has 5 minutes to present their recommendations and rationale.
  - Allow 2–3 minutes for questions and discussion after each presentation.
  - Encourage discussion from the other participants (within time limits).
- Tell participants during debrief to look at their own country's emergency management organization to use as a reference to be able to generate a resilience plan.

Topic: Module Summary	**10 Minutes**

Slide 36 Module Summary
▪ Critical infrastructure resilience ▪ Critical infrastructure security and resilience policy example ▪ Planning for resilience
Graphic Description: No Graphic

- Summarize the module by reviewing the following points:
  - **Critical infrastructure resilience**
    - Resilience — to prepare and adapt, withstand and recover rapidly.
    - Collaboration — to work together to achieve shared goals.
    - Protection — the capabilities necessary to secure the homeland.
  - **Critical infrastructure security and resilience policy example**
    - Integrates prevention, preparedness, response, recovery
    - Introduction
    - Policies
    - Roles and responsibilities
    - Strategic imperatives
    - Innovations and research and development
    - Actions to implement the directive
  - **Planning for resilience**
    - Determine where resilience is adequate
    - Determine where resilience is deficient
    - Develop a plan that will help ensure recovery and resilience occur in a timely manner
    - Gap analysis process s— four-step process
    - Proposed security countermeasures
    - Identify and prioritize recommendations
    - Develop a national operational resilience plan that integrates prevention, preparedness, response, and recovery
- Ask whether there are any questions about the contents of this module.
- Explain that in *Module 16: Capstone Exercise* participants will have the opportunity to apply the concepts and procedures for evaluating the physical protection system of a selected critical infrastructure.