THREADED EXERCISE WORKBOOK

Threaded Exercise Workbook....1
Introduction to the Threaded Exercise (Module 5)....3
Part 1: Critical Infrastructure Components (Module 5)....6
Part 2: Critical Infrastructure Assets (Module 6)....41
Part 3: Threat Analysis (Module 10)....49
Part 4: Bomb Threat Management Policy (Module 11)....64
Part 5: Security Force Operations (Module 12)....68
Part 6: Security Technology (Module 13)....71
Part 7: Security Inspection and Validation (Module 14)....76
Part 8: Operational Resilience Plan (Module 15)....82

This Page Intentionally Left Blank.

INTRODUCTION TO THE THREADED EXERCISE (MODULE 5)

Vulnerability analysis is a complex and multi-step process. To facilitate your understanding of the process, this exercise has been designed as a **threaded exercise** — a scenario-based progressive learning activity that builds upon the learning objectives outlined in the modules in which the exercise occurs. Because of this design, you must complete each part of the exercise in the prescribed sequence:

Parts of the Exercise	Complete After
Part 1: Critical Infrastructure Components *1.1 Conduct Vulnerability Analysis Team Assignment* *1.2 Prepare for the Data Call* *1.3 Complete a Review of the Data Call Information* *1.4 Develop Questions for Each Critical Infrastructure Component*	*Module 5: Critical Infrastructure Components*
Part 2: Critical Infrastructure Assets *2.1 Identify Critical Infrastructure Assets and Loss Analysis* *2.2 Create Threat Spectrum Matrix*	*Module 6: Critical Infrastructure Assets*
Part 3: Threat Analysis *3.1 Prepare the Threat Analysis* *3.2 National Ministries Building Data Collection*	*Module 10: Analyzing the Threat*
Part 4: Bomb Threat Management Policy *4.1 Bomb Threat Management Plan Considerations*	*Module 11: Policies and Procedures*
Part 5: Security Force Operations *5.1 Develop Security Force Plan*	*Module 12: Security Force Operations*
Part 6: Security Technology *6.1 Develop a Security Technology Plan* *6.2 Finalized Threat Analysis Statements*	*Module 13: Security Technology*

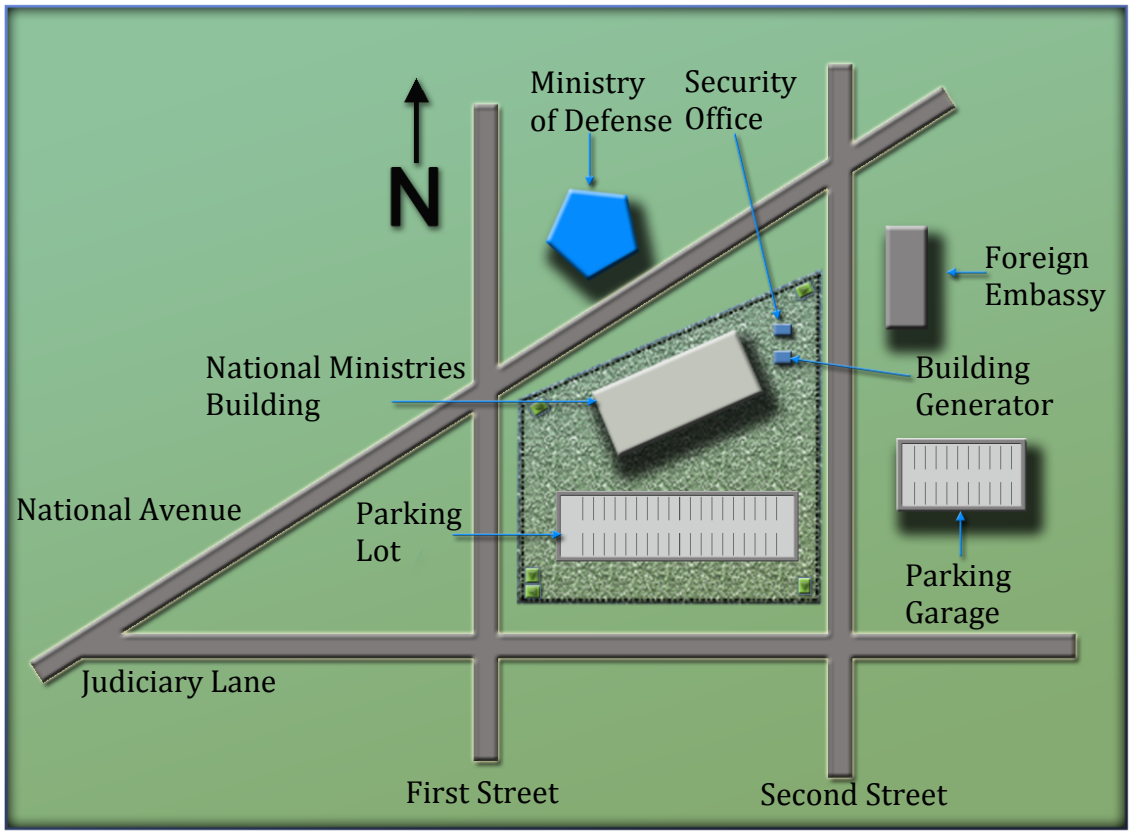
Parts of the Exercise	Complete After
Part 7: Security Inspection and Validation *7.1 Develop the Security Inspection and Validation Checklist*	*Module 14: Security Inspection and Validation*
Part 8: Operational Resilience Plan *8.1 Develop Operational Plan Security Countermeasure Recommendations*	*Module 15: Operational Resilience*

Introduction to the National Ministries Building Scenario

Although the exercise is divided into eight parts, with each part relating to a specific learning objective, all parts of the exercise share the same scenario:

> Your team has received a request from the Head of State's Chief of Security to conduct a vulnerability analysis of the primary government facility — the National Ministries Building — which houses the Head of State, her ministries, and the country's National Museum.

As you proceed through each module, you will receive additional information to use to make decisions in the analysis of this government facility. Remember, you will not receive all information immediately. Keep your completed notes on each module for reference in the following modules.


N
Ministry of Defense
Security Office
Foreign Embassy
National Ministries Building
Building Generator
National Avenue
Parking Lot
Parking Garage
Judiciary Lane
First Street
Second Street

PART 1: CRITICAL INFRASTRUCTURE COMPONENTS (MODULE 5)

General Directions:

In order to complete this part of the exercise, you will have to complete the following activities:

- Finalize vulnerability analysis team assignments
- Prepare for the data call
- Complete a review of the data call information
- Develop questions for each critical infrastructure component

There are specific directions for each of the activities. Be sure to read the directions carefully. If you have questions, ask your facilitators for guidance.

1.1 Finalize Vulnerability Analysis Team Assignments

In the planning phase, begin by designating a project manager and identifying the area of experience for each member of the vulnerability analysis team. Remember, at a minimum, an effective vulnerability analysis team should consist of the following positions or roles:

- Project manager — coordinates and assigns tasks as required
- Security system technologist(s) — provides expertise regarding the security measures that could be deployed at the site
- Threat assessment subject matter expert(s) — provides insight and expertise about the threat assessment process
- Facility subject matter expert(s) — provides accurate data about the site and specific operations; also expedites the vulnerability analysis team's ability to arrange site tours, identifies individuals to be interviewed, and assists in completing the analysis

Purpose:	To evaluate the critical infrastructure components of the National Ministries Building
Reference:	Module 5: Critical Infrastructure Components
Duration:	90 minutes (70-exercise; 20-debrief)
Group composition:	Table groups
Debrief:	Presentations and discussion
Equipment:	National Ministries Building Complex Map

Directions:

1. Within your team, discuss the experience level of the vulnerability analysis team.
2. Appoint a project manager and assign each member of your team to a role. While you will usually have only one project manager, you may have multiple technologists or subject matter experts.
3. Use Table 1: Vulnerability Analysis Team Assignments to list the name and role of each team member.
4. You have 10 minutes to complete this segment of the exercise.
5. Be prepared to share your responses with the class.

Table 1: Vulnerability Analysis Team Assignments

Name	Role/Area of Expertise
	Project Manager

1.2 Prepare for the Data Call

It is now time to request a data call from the point of contact at the National Ministries Building. In preparation for the data call, your team will compile a list of the information you will need to conduct the site visit. While you will not be physically conducting the site visit during this exercise, you still must gather the necessary information to complete this important task.

Directions

1. Using the space provided beneath each of category headings below, write down the types of information your vulnerability analysis team would like to have. This task is completed prior to conducting the site visit.
2. Refer to the information from **Addendum 5.2 Gathering Component Data** provided below to help you identify what is needed.
3. Your team has 15 minutes to complete this segment of the exercise.
4. Be prepared to share your responses with the class during the debrief session.

Physical Conditions

- Maps of the facility and topography
- Detailed site maps and drawings showing building locations and critical asset locations
- Interior facility drawings indicating critical asset locations and security system components, such as fences, alarms, and closed-circuit television cameras
- General information about climate and annual weather conditions

Facility Operations

- Information that illustrates the facility's mission and critical assets
- Schedules of work activities to include open and closed periods involving critical assets
- Schedules of security force personnel to include numbers of personnel based on work schedules and shift changes

Facility Policies and Procedures

- Facility policies and procedures related to:
  - The security force, such as standard operating procedures and protection strategies
  - Access control and visitors
  - Performance testing security measures
  - Reporting unusual occurrences
  - Protecting critical assets
  - Past reports on violations related to facility security
  - Protecting information technology

Regulatory Requirements

- Regulations from the government authority responsible for the specific critical infrastructure
- Local emergency services response regulations
- Government mandated security regulations
- Past reports on regulation violations

Safety Considerations

- Evacuation plans affecting critical asset area
- Safety inspection reports concerning critical asset areas
- Emergency services response plans to critical asset areas

Legal Considerations

- Information concerning lawsuits at the facility that relate to:
- Security force personnel, policy, and procedures
- Searching of employees and visitors to the facility
- Failure to provide proper training issues
- Failure to comply with regulatory requirements
- Any information on the final outcome of such legal issues

1.3 Complete a Review of the Data Call Information

The site point of contact received your team's request for information and sent a letter of response. In preparation for the site visit, you need to review this letter, discuss the information provided, and identify any information that might be missing or you have additional questions about.

Directions:

1. Read the section titled Facility Director's Response Letter and all attachments.
2. Discuss the types of information received.
3. In the space provided beneath the section titled Data Review:
   a. List all the information that your team thinks will be relevant for the vulnerability analysis.
   b. Identify any information that may be missing.
   c. List any clarifying information you may need before the site visit.
4. Your team has 30 minutes to complete this segment of the exercise.
5. Be prepared to share your responses with the class.

Data Review

Facility Director's Response Letter

National Ministries Building
National Avenue
Capital City

To: Vulnerability Analysis Team

In response to your request for data, I have provided the following information. Please contact me if you have any questions.

Description:

The National Ministries Building was completed in early 1985 and is the third of three office buildings constructed to house government operations in the area. It occupies a site south of the National Military Building bounded by First and Second streets on the west and east with National Avenue on the north.

The design of the building is a rectangular plan with three stories above ground. One story that is half the size of the above-ground structure is underground and is used as a loading dock area. The building is built with a concrete and steel frame and a red brick façade. Each above-ground floor is approximately 2,973 square meters with the loading dock area occupying about 1,394 square meters.

The building houses the Head of State, her staff, and eight ministers and their staffs. The National Museum occupies half of the first floor of the building.

The ministries include:

- **Ministry of Commerce** — Responsible for quality control of food supply, consumer protection, companies and commercial agents, and related industries like tourism
- **Ministry of Defense** — Oversees the Army, Air Force, construction of military bases, and civilian airports
- **Ministry of Transportation** — Responsible for all means of transportation to include air and land, as well as regulations associated with both government and private-sector agencies
- **Ministry of Health** — Provides all health-related information and care to the country's citizens
- **Ministry of Taxation** — Collects taxes and maintains comptroller responsibilities for the country
- **Ministry of Resources** — Maintains control over the country's resources to include power, agriculture, manufacturing, minerals, and so on
- **Ministry of Justice** — Provides law enforcement services, prosecution and judicial services, and oversees the prison system
- **Ministry of Interior** — Maintains public security, national and international intelligence, and special security and investigation

Each minister maintains an office in the building with the Ministry of Interior being the largest office in the building.

The National Museum tells the story of the fight for freedom and contains over 100 pieces of art from the period of the struggle, to include 50 irreplaceable artifacts. The museum is open to the public Tuesday through Sunday from 1000 to 1800. Museum staff members are not present on Monday when the museum is closed.

Physical Conditions

I have provided maps and diagrams attached to this letter for your reference.

- Map #1 depicts the area near the National Ministries Building.
- Map #2 is the plot plan for the National Ministries Building and other structures within the fence line.
- Drawings #1, 2, and 3 are floor plan layouts; the loading dock floor plan is not available.

Seasonal weather conditions vary as follows:

- November–March the ground is covered in 25.4–30.48 centimeters of snow with temperatures averaging around 0 degrees Fahrenheit (-17 Celsius).
- April–May is spring weather with the temperatures averaging around 55 degrees Fahrenheit (13 degrees Celsius) with significant rainfall.
- June–August is summer time with the temperatures averaging around 85 degrees Fahrenheit (29 degrees Celsius) with the potential for 100 degrees Fahrenheit (38 degrees Celsius) days and moderate rainfall.

- September–October is the fall time of the year with temperatures averaging around 45 degrees Fahrenheit (7 degrees Celsius) with moderate rainfall.

Facility Operations

The primary mission of the National Ministries Building is to house the senior executive staffs of the government. It also serves as an information source through the National Museum and provides a visible icon for national pride. With the exception of the Ministry of Interior, all other Ministries have other government buildings in which they conduct their operations.

The operational work schedule of the building is normally 0800 to 1700, Monday through Friday. There are about 1000 employees working the normal daily schedule with weekends and holidays off. At 1600, 200 employees arrive at various ministries for an evening shift. Among that group are janitorial and security service personnel. At 2400, when the second shift ends, an additional number of people arrive to work at the Ministry of Interior; the exact number was not available when questioned.

Security Force Personnel

Security force is a military style organization with a similar hierarchy. The Chief of Security oversees each site Captain and their staffs. The following policies and procedures apply to the security force:

In the event an emergency occurs, all available security force personnel will report to a designated area and await direction from the senior security force member on duty.

All security force members are required to complete the 15-week Protective Force training academy before being allowed to work alone. This training must be completed within one year of employment. Past violations by security force personnel include sleeping on duty, drug abuse, and inappropriate use of force.

Access control is not automated; security force members physically check identification badges as employees enter the building. Individuals not possessing a badge must stop and obtain clearance from a sponsor before proceeding into the building. Visitors to the museum must enter through the north entrance and sign-in at the security desk before proceeding to the museum unescorted. Restricted areas are locked and only authorized personnel are issued keys.

Performance testing is conducted at the firing range annually when security force members qualify. Testing of security technology countermeasures is not conducted. At the direction of the shift lieutenant, reports of unusual events are completed; last year 20 reports were completed.

The Chief of Security believes that the building contains hundreds of assets that include

personnel, information, equipment, and processes.

Regulatory Requirements

The physical security policies and procedures developed by the Ministry of Interior and the National Regulatory Agency are attached.

Since the requirements issued last month, the National Ministries Building has not undergone an evaluation of the facility.

Security Force Personnel Demeanor

Security force is a military style organization with similar standards including:

- **Dress Code**: Uniforms will be clean and pressed for duty. Equipment must be complete and shoes polished.
- **Weapons**: Each security force member will carry the issued weapon(s). There is no exception to the types of weapons carried.
- **Code of Conduct**: Each security force member will conduct themselves in such a way as to bring honor and distinction to themselves and the organization. Any member who violates the code will be subject to discipline.

Security Force

Security personnel provide security 24 hours a day, 7 days a week, and 365 days a year at the National Ministries Building. The following are assignments for each security force member:

Position	Location	Work Schedule	Hours
Captain (1)	Security Office	Monday–Friday	0800–1700
Lieutenant (3)	Security Office	1 each shift includes weekends and holidays	All periods
Sergeants (3)	Security Office and Roving	1 each shift includes weekends and holidays	All periods
Post #1 Fixed Post (2)	North Entrance	Tuesday–Sunday	1000–1800
Post #2 Fixed Post (3)	South Entrance	1 each shift includes weekends and holidays	All periods

Security Control Center (3)	Security Office	1 each shift includes weekends and holidays	All periods
Patrol (3)	Roving	1 each shift includes weekends and holidays	All periods

Safety Considerations

Rehearsal of emergency evacuation is conducted annually for each shift of employees and visitors. Evacuation routes are posted throughout the building.

The last fire extinguisher checks were 15 days ago. I am not sure what "critical asset" area means, but all areas receive the same consideration for safety.

The National Police, Fire Service, and Rescue Service Emergency provide emergency services. The nearest station is located 3.2 kilometers from the National Ministries Building.

Legal

Use-of-force rules prohibit security force members from using more force than necessary to accomplish the task. Use of nonlethal force weapons is not available to security force members.

It is legal to search anyone who enters a government facility. Employees are not searched if they possess government identification. Visitors' bags and parcels are randomly searched when they enter the facility.

One use-of-force lawsuit has been filed with the country's Attorney General's Office from an incident three months ago, when a security force member arrested a protestor and broke his arm. The security force member was suspected of excessive use of force; the investigation indicated that the member was in violation of policy.

Respectfully,

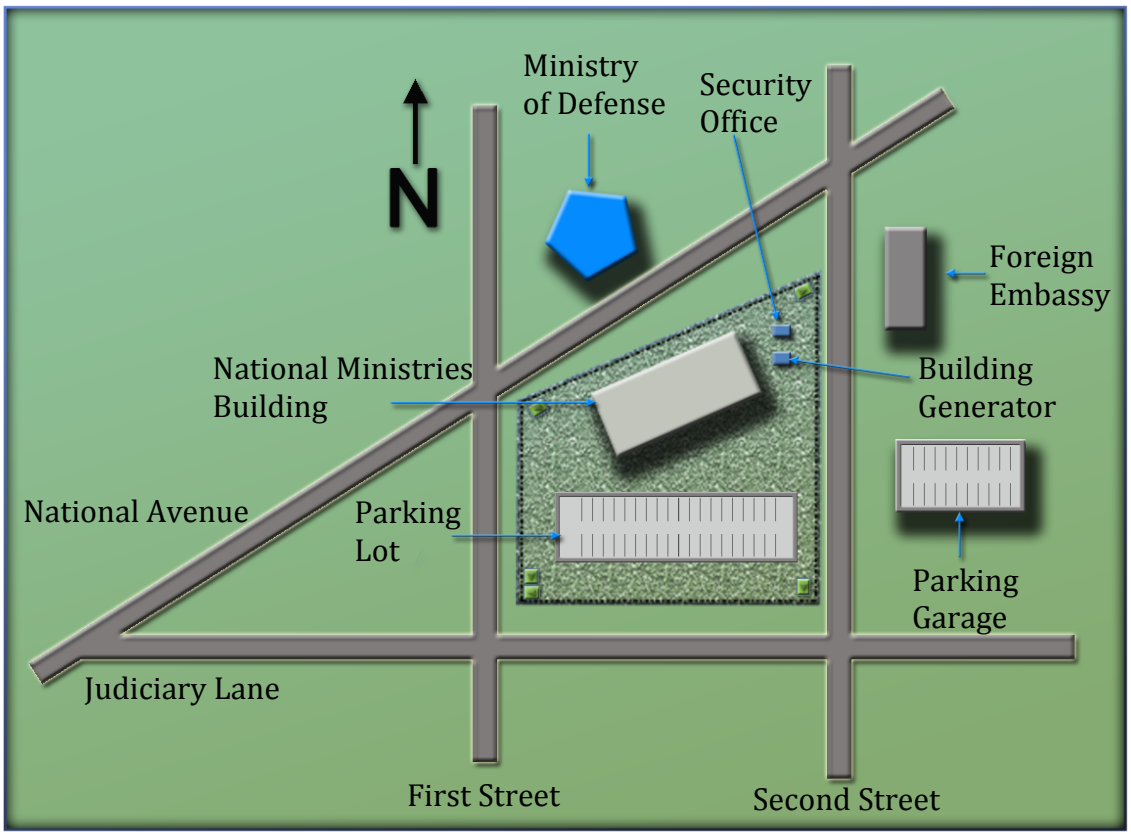
Charles J. Lewis

Facility Director

National Ministries Building

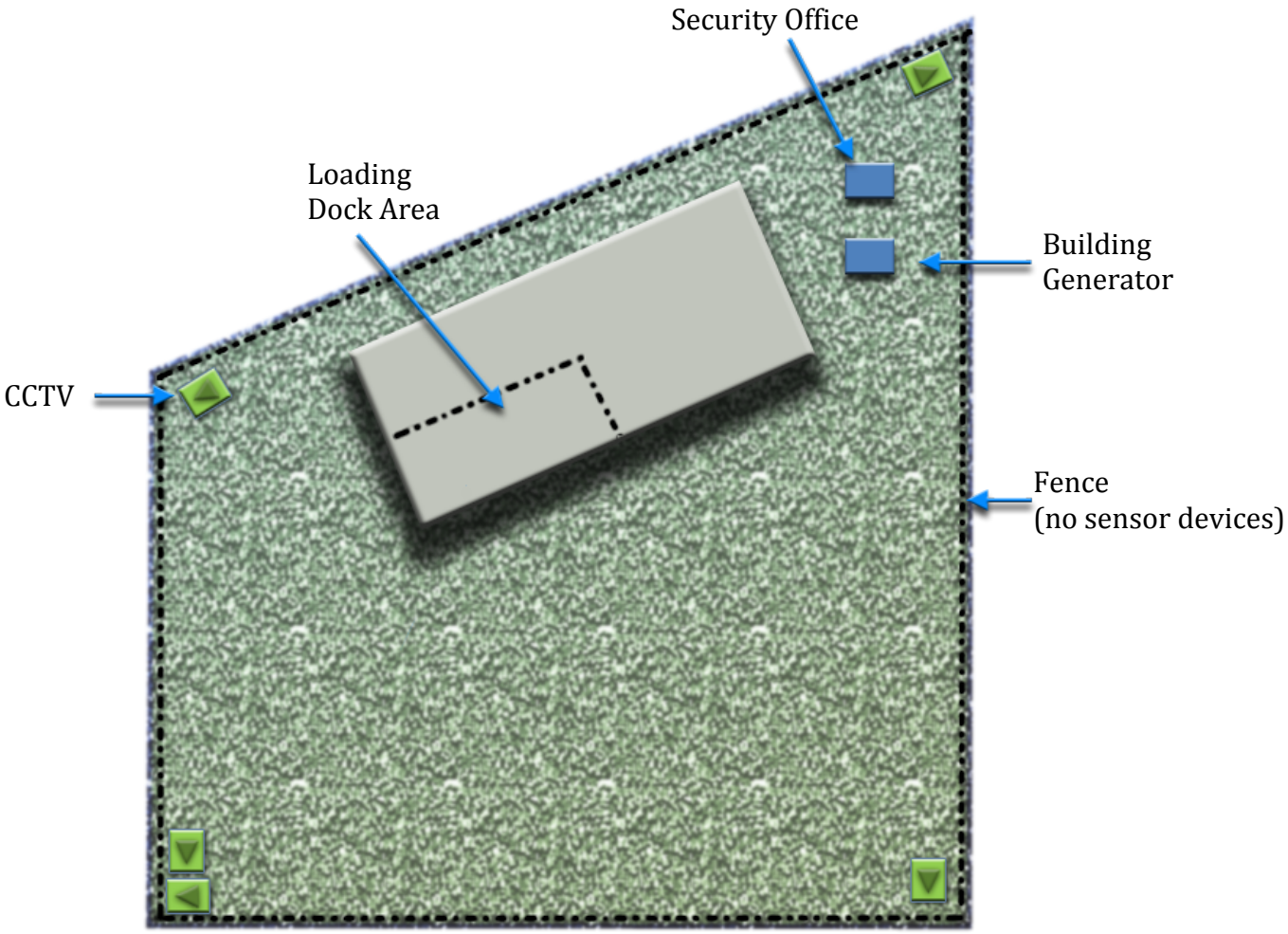
Attachment 1: Map of Area near National Ministries Building

Map #1: Area near National Ministries Building



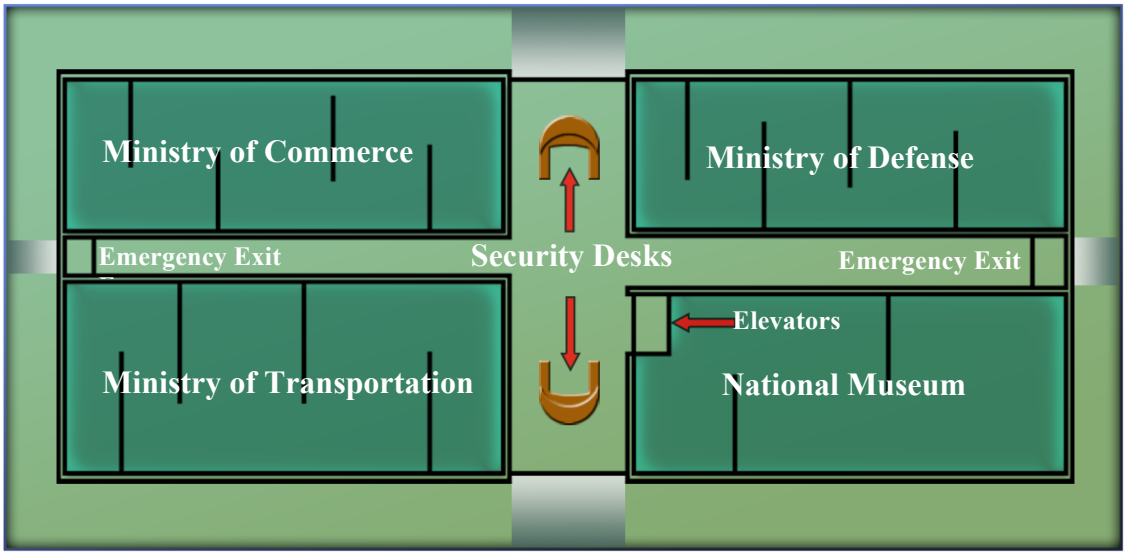
Attachment 2: National Ministries Building Plan with Security Controls

Map #2: Plan with Security Controls



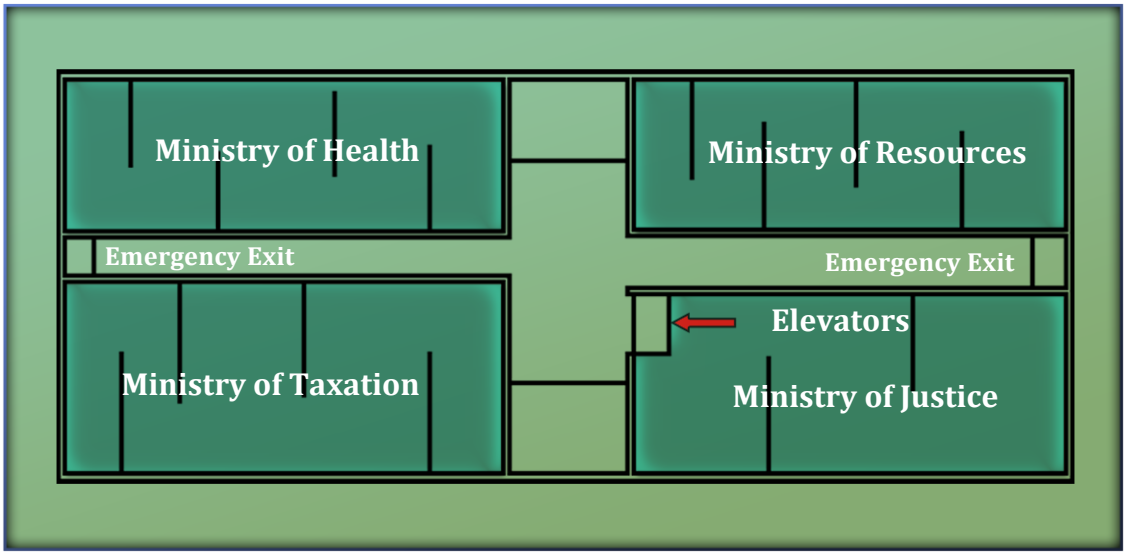
Attachment 3: National Ministries Building Floor Plan of First Floor

Drawing #1: First Floor



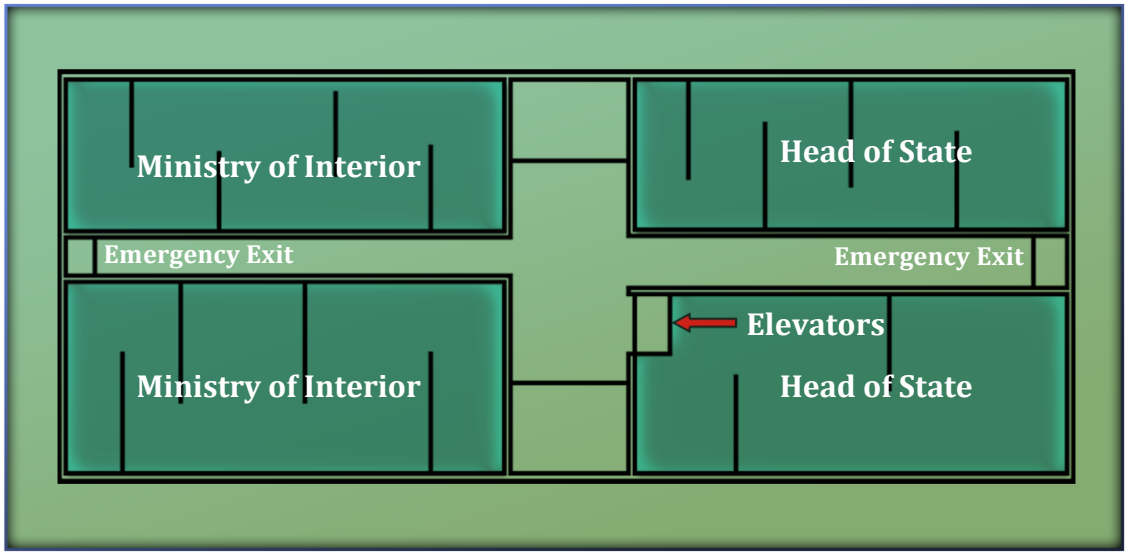
Attachment 4: National Ministries Building Floor Plan of Second Floor

Drawing #2: Second Floor

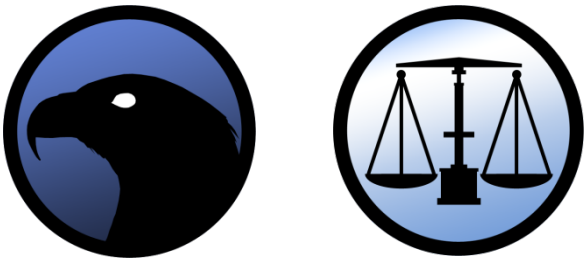


Attachment 5: National Ministries Building Floor Plan of Third Floor

Drawing #3: Third Floor



Attachment 6: Physical Security Policies and Procedures



Introduction

The following represents the baseline physical security requirements for government facilities. The information is provided as a guide to assist management in determining the minimum physical security requirements for implementation. The data was compiled from existing regulatory documents dealing with physical security instructions, physical security system specifications, and industry standards. The question of minimum standards can be difficult to address across a wide range of facility functions and potential threats, but the concepts associated with providing standard requirements can be addressed as depicted in this document. The physical security measures applied to government facilities generally include:

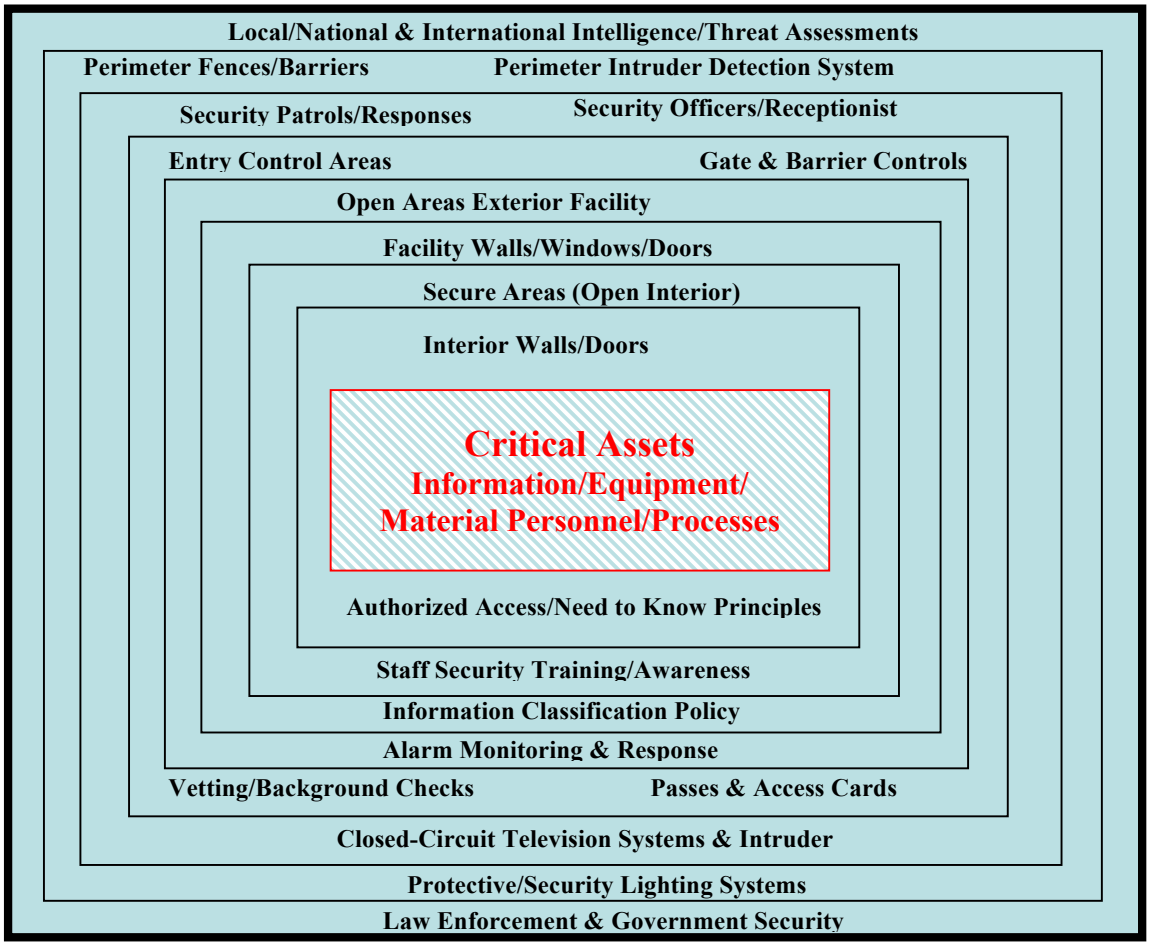
- Policies and procedures
- Perimeter barriers
- Lighting
- Intruder detection systems
- Closed-circuit television
- Automated access control systems
- Security officers and patrols
- Lock and key controls
- Entry control areas
- Secure asset locations

Protection in Depth

Effective protective security results from a carefully planned system of security measures designed to protect information, equipment, material, personnel, activities, and facilities. These controls must form an interdependent and interlocking series of defenses arranged in depth and outward from the asset(s).

The physical security measures chosen as a result of a vulnerability analysis should be arranged so as to be mutually supporting. Security measures must be practicable and cost effective (see *Figure 1: Protection In-Depth Strategy*).

Figure 1: Protection In-Depth Strategy



Vulnerability Analysis & Threat Assessment

Due to the uniqueness of each government facility, each government facility shall undergo a vulnerability analysis by a qualified team of subject matter experts.

Baseline Physical Security Measures

The following table illustrates the baseline physical security measures for government buildings and provides specific information concerning each of the mandatory and recommended security measures.

Government Buildings Physical Security Measures			
Protection in Depth Element	Security Measure	Mandatory or Recommended	Comments
Facility Perimeter	Fence, natural landscape, gates, security officers with Perimeter Intruder Detection Systems and closed-circuit television	Highly Recommended	May not be feasible at all locations
Open Areas Exterior Building	Lighting for parking lots and walkways, closed-circuit television, and security patrols	Mandatory	Security patrols as directed by local post orders
Facility (Building) Entrances	Automated access controls, security/receptionist visitor controls, closed-circuit televisions, doors and windows secured, identification cards	Mandatory	All controls should be applied, if variance required, variance should provide equal to or better protection
Open Areas Interior	Authorized badges displayed, visitor escort, security patrols and closed-circuit television at entrances into controlled areas	Mandatory	Security patrols as directed by local post orders, visitor escort by authorized personnel only
Controlled Areas (Ministries Restricted Areas, Head of State Office, and Others as Designated)	Controlled access list, automated access controls, security patrols, closed-circuit television within controlled areas	Mandatory	Additional requirements may be mandatory based on client requirements, e.g., government security clearances

National Security Measures

Policies and Procedures

Establish a set of policies and procedures that outline the roles and responsibilities of security force personnel and should reflect the general requirements as directed by the Chief of Security. Each policy should be reviewed annually and revisions completed in a timely manner. A good security policy includes a simple introduction that conveys the purpose of the policy, the policy statement itself, and information about how compliance will be measured. It should also include information about what sanctions will be taken against those that fail to comply.

At a minimum, the Security Policies and Procedures Manual should contain the following elements:

- A description of the facility site, to include general functions, number of personnel at the facility, employees, contractors, and visitors
- A floor plan of the facility, that identifies critical areas, security countermeasure locations and emergency evacuation routes
- A description of access controls and how they are applied to the facility; for example, card access with additional personal identification numbers for critical areas for specified personnel. The description should include the procedure of granting visitor access as well as escort responsibilities
- Security force policies and procedures must outline in detail their responsibilities in performing their assigned functions; such functions include conducting patrol activities, maintaining assigned posts, dealing with the public, and reporting unusual occurrences

Perimeter Barriers

A perimeter barrier can be defined as a natural boundary, free-standing fences or walls, the outer walls of a building or the divisions within it. Its function is to provide a degree of physical, psychological, or legal deterrence to intrusion. Its effectiveness as a security measure can be enhanced by the deployment of Perimeter Intruder Detection Systems, closed-circuit television, security lighting, and security officers.

Ideally, a fence should enclose the entire operational area. When this is not practical, enclose individual key areas, as feasible. If possible, multiple facilities should be grouped together to ensure an efficient and effective means of providing coordinated security. The purpose is to provide the first level of protection to a key facility.

When a fence is not feasible, use natural landscape and other constructed material to identify an appropriate boundary for the facility. The purpose of any perimeter barrier should be to:

- Designate (outline) a boundary
- Channel visitors to legal points of entry

- Deter and delay unlawful intruders

For the barrier to be effective in deterring intruders, the following standards should be applied:

- Surveillance of the barrier should be conducted by either members of the security force or closed-circuit television.
- If feasible, alarm the barrier with some form of intrusion detection.
- Apply suitable security lighting to the area. Ensure that the barrier(s) is well maintained and vegetation in and around the area is clear.

If a fence serves as the barrier, anticlimbing devices such as barbed wire outriggers may be used. If the area is controlled by a vehicle gate(s) that allows access through the gate by card reader and security officer monitoring, the remaining fence perimeter must be secured at the same level, to include controlled pedestrian gates, or secured when not in use. Apply appropriate "No Trespassing" signage to perimeter boundaries.

Due to the variety of building configurations, the exterior walls, doors, and windows of the facility may serve as the initial barriers. In those situations, the following minimums apply to the facility:

External Door Construction

The following standards should be used for external door construction:

- Install external doors that are made of solid hardwood or metal, solid laminated core or solid multi-ply construction.
- Strengthen solid softwood doors, where already fitted, by fitting a steel plate over the outer face of the door.
- Configure external doors to open outwards, because these are more difficult to force.
- Cap external door hinges to prevent pin removal.
- Ensure doors are close-fitting and equipped with suitable locks.
- Install locking bars across the back of the door to offer an extra layer of protection.
- Seal or otherwise protect letter boxes.

External Doors No Longer in Use

Brick up or permanently secure external doors that are not used and that are not emergency exits by screwing a steel sheet across the inside of the door frame, which should be securely bolted to the building material.

Glazed Doors

Strengthen glazed or semi-glazed doors by fitting a steel mesh grille to the doors. Alternatively, install expanding grille gates or steel roller shutters behind the doors. If it is a specially-designed door where unobtrusive protection is desirable, the replace glass by security glazing material.

Double Doors

Fasten double doors by bolts attached to the first closing leaf of the door (at the top and

bottom) and a security deadlock, preferably fitted with a hook-bolt attached to the other leaf. Double doors that are not final exit doors can also be fitted with internal cross bars and the second closing leaf secured with barrel bolts.

Inter-Connecting Doors

Doors connecting to other parts of a building under separate occupancy should, in general, provide a degree of security similar to that of external doors.

Internal Door

Where there is a requirement to keep doors to the basement, ground, or first floor rooms locked, the keys to the locks on such doors are to be held under secure conditions, but are to be readily accessible to authorized persons.

Security of Emergency Exit Doors

While escape routes are essential, recognize that emergency exits do represent a perimeter weakness. Fire exits should be fitted with intruder detection systems/alarms and within a robust, approved locking mechanism that conforms to fire regulations. Liaison with the fire department is essential in meeting these requirements.

Emergency Exit Standards

Fire exit doors must comply with fire regulations of the local area, to include international standards.

Door Frames

The following applies to door frames:

- Where the security of a door depends, in part, on its frame consider strengthening the frame and its attachment to the surrounding building material.
- Where required, reinforce doorsteps by replacing wooden sills with concrete.
- Where frames are secured by nails driven into the brickwork, they can be fitted with steel supports on both sides of the frame and attached by steel brackets to the masonry for greater security; alternatively, expanding bolts can be used, provided that they are set deep into the brickwork.
- Where the building material is not suitable for bolts or steel brackets, consider additional physical security measures (closed-circuit television, intruder detection systems).

Door Bolts

The following applies to door bolts**:**

- Use door bolts in conjunction with security locks and fitted in pairs (at the top and bottom of the door).
- Ensure that bolts cannot be opened from outside the door and that the fixing and strength of the staple are adequate.
- Ensure that the bolt engages into the floor fully and keep the hole in the floor free from obstruction.
- Use pad bolts with security padlocks to secure doors on a more permanent basis.
- Carefully select bolts for double doors.

- Fit flush bolts for double-rebated doors into the edge of the first closing half of the door so that they are completely covered by the half of the door. For double doors without rebates, fit flush bolts with turnover levers in the same way.

Grilles & Shutters

Use expanding grille gates, roller grilles, or roller shutters in doorways, passages, or other openings. Use these as a second layer of defense behind existing external doors, especially where there is a threat of forcible attack. Grilles may be useful in hot climates where a closed solid door is undesirable. The frames of grilles or shutters should be well secured to the surrounding structure of the building and preferably should be inaccessible from the outside of the building.

Windows

The following security points regarding windows apply:

- Brick up or otherwise secure all accessible nonessential windows.
- Install secure fittings to all basement, ground floor, and other windows that are readily accessible.
- Examine window catches and replace defective catches.
- Consider providing intruder alarms for protection.
- Identify responsibility for securing windows with potential access from ground floor level or reasonable climbing heights in the local security instructions. Ground floor windows and those that are easily accessible to entry must have locking handles or opening restrictors.
- Consider installing bars, grilles, or shutters where it is necessary to secure a window more effectively than by the use of a lock, catch, or bolt. Also, consider the installation of intruder detection sensors.
- Apply double glazing to provide additional protection against secret attack and some protection against forcible attack. Double glazing can be alarmed and has the further advantage of thermal insulation and noise reduction. The frame of the glazing material should not be accessible from the outside.

Roofs

For roof areas, the following applies primarily for establishments in urban areas or buildings housing sensitive information or equipment:

- Survey roofs to see whether there is access onto them from adjoining buildings, nearby buildings, trees, fire escapes, or window cleaning equipment. If there is the potential for access, it may be necessary to erect suitable barriers. Fit intruder alarms, if access is necessary, for example, as part of a fire escape route.
- Incorporate suitable measures to protect access to a building via an attic or roof space.
- Block off access from a roof into a building via a chimney by, for example, inserting a grille.
- Secure roof access doors in the same way as other external doors if the roof is accessible from neighboring buildings or from the ground.

Skylights, Fanlights, Roof Lights

It is possible to secure skylights, fanlights, and roof lights with locks or bolts. When more

protection is needed, however, one of the following is to be considered:

- Replace the glass with security glazing material.
- Fit with bars or grilles.
- Screw the frames in place and cover the glass with steel mesh secured to the frame on the inside.
- Install intruder detection system.

Downpipes

The upper floors of a building or from the roof may often be accessible by way of rainwater or soil downpipes. Such access can be restricted by boxing in the pipes or by treating them with anticlimb devices.

Sunken Outside Areas

Buildings, not within the confines of the facility boundary, can have sunken external areas at basement level, which are accessible from the street. These can provide cover for persons seeking to gain entry through basement windows and afford convenient sites for depositing explosive or blast incendiary devices. The following is to be considered for the establishment's security:

- Secure steel grilles or steel mesh screens from below, providing that these do not enable easy access to the building.
- Fit vents into sunken areas or vents emerging at street level with internal steel grilles.
- Install padlocked crossbars fitted on the inside to prevent access through service tunnels.
- Install intruder detection system.

Loading Docks

Consider the following for parking or loading bays under a stand-alone building in an urban area:

- Outside working hours, they should be closed with roller shutters or sliding shutters secured on the inside.
- During working hours, the bays should be monitored by area custodian or closed with electronically operated shutters that are only opened when the incoming vehicle has been identified.

Public Utilities

Gas, electricity, and water supply installations within buildings may offer potentially vulnerable access points, particularly in stand-alone buildings in urban areas. Where possible, cables and pipes are to enter the building underground and should be restricted from access. If anyone could gain unauthorized access through these access points, consider installing grating and intruder detection systems. Site public service meters so that access to them does not require entry into sensitive areas.

Air Conditioning and Other Support Systems

Where air conditioning is essential to equipment operation (such as computer installations), give adequate protection to the electricity, and water supply for the air conditioning system. If sabotage is a threat, additional security measures may be required.

Multi-Occupancy Buildings

Where there are occupants of a building other than government agencies, other tenant organizations should secure their portion of the building at the same level as the government, or ensure that the security measures applied to the government facility consider the existing tenant security levels.

Lighting

All vulnerable external areas should be well lit, particularly car parks, access routes (both pedestrian and vehicular), and building entrances. Provide lighting to all external doors, with timing devices for daytime and nighttime conditions. Similar provisions are required to serve common entrances and multi-occupancy buildings as detailed above. Lighting sources must be compatible with the requirements of closed-circuit television. (For example, low pressure sodium vapor is not compatible with closed-circuit television.)

Perimeter Lighting

Design perimeter lighting is to cast a uniform light on the perimeter. Overhead lamps or low-mounted lamps provide uniform light that creates a glare effect to dazzle and deter intruders. If the latter are used, they are not to create a nuisance or hazard outside the perimeter. Design the lighting so that it does not reveal the position of patrolling guards. Avoid lighting security posts or reception rooms so that security officers can be seen or silhouetted.

Area Lighting

Area lighting is to illuminate areas inside the perimeter that intruders must cross in order to reach their objectives. Such lighting increases the security officers' ability to detect intruders and acts as a powerful deterrent. The illumination should be even and without shadows.

Intruder Detection Systems

Intruder detection systems are designed to detect the entry, or attempted entry, of an intruder into a protected area, to identify the location of the intrusion, and to signal an alarm to a security force. When correctly installed, performance-tested, and employed, an intruder detection system can result in savings in security manpower. To be effective, an intruder detection system must have a security force that will react in the event of an alarm condition. An intruder alarm does not delay an intruder; it only detects the intruder's presence. It is only effective if the security force arrives in time to prevent the intruder from achieving his or her purpose. The intruder alarm system is best used to give early indication of the attack. It is, therefore, imperative that the signal notifying the attack is safely transmitted to a central security control room for the security force to initiate action. To assist the security personnel in verifying the intrusion, the intruder systems should have a combination of perimeter, trap, and point protection:

- **Perimeter protection** usually refers to the devices activated by intrusion or attack upon the perimeter.
- **Trap protection** describes those devices activated once the intruder is inside the building.

- **Point protection** describes those devices that are used to protect high value and portable items.

Using a combination of these three approaches is usually the most effective way to provide the required verification of an incident and to achieve effective and in-depth security. Correctly positioned closed-circuit television cameras will aid in alarm verification.

For unmanned facilities, an intruder detection system should be installed with all of the following:

- Door contact sensors as a minimum requirement
- Sensors reporting to a security control center
- Access control function provided by the security control center
- Verification by security or law enforcement personnel to unannounced sensor activation or other unusual occurrences

Alarm Display and Signaling

Alarms may be signaled by audible means with closed-circuit television integration that requires the area of the activation to be immediately visible on a security monitor. For remote sites, the sensor signal should report to a permanently manned control position and may indicate a loss of power, tampering, or an open door.

Closed-Circuit Television

The use of closed-circuit television for surveillance may save manpower, especially when used in conjunction with an intruder detection system and automated access control system. It may also supplement, extend, and make more effective an existing security system. Closed-circuit television enhances the effectiveness of perimeter security, particularly if used to verify the alarms signaled by perimeter intruder detection system.

Closed-circuit television is **not** a security detection device unless used with video motion detection. It is a generally considered to be a management tool for alarm verification. Closed-circuit television does provide a valuable function in that it can:

- Make security personnel more effective and can be used to direct responses and assist in the control of incidents.
- Be a deterrent to intruders.
- Assist in post-event analysis and incident investigation.
- Assist with entry control.
- Provide general operational information to aid in running the premises.
- Provide site monitoring at night.
- Be fitted with video detection capability; consider using it to monitor the external areas to the facility.
- Be used for alarm verification.

Selecting closed-circuit television cameras and their performance specifications is dictated by the requirements of the specific site. Closed-circuit television application depends on the expectations of the system. General monitoring of large areas is not sufficient to recognize a known individual or vehicle license plates. Identification of an individual or

license plates requires increased focal views. Identify facility expectations in the design of the physical protection system.

The government requires that closed-circuit television cameras be a part of the physical protection system and that cameras be deployed in areas where they achieve the following standards:

- Place closed-circuit television cameras to monitor the main entrance for entry and exit surveillance **(Identification).**
- Use a camera at each external access control point and in conjunction with an intercom if direct viewing of visitors is not possible **(Identification).**
- All access-controlled perimeter barriers should be supported by use of intercom and Closed-circuit television camera **(Recognition)**.
- Closed-circuit television cameras should provide surveillance of the facility perimeters with no gaps **(Recognition).**
- Closed-circuit television cameras should view car-parking areas **(Recognition)**.
- Cameras must be placed to monitor the entrance and exit from critical areas and secondary areas such as uninterrupted power supply and security control center, the heating and ventilation supply, switching rooms and build rooms **(Identification).**
- Closed-circuit television cameras should provide internal area surveillance **(Recognition).**
- Lighting must be adequate to provide a clear image.
- Install closed-circuit television systems with video motion detection, where necessary.
- All installed and properly maintained closed-circuit television systems must be monitored on a 24-hours-a day, 7-days-a-week basis, and an appropriate trained force must be available to respond to any identified alarms or incidents. The system should be capable of being remotely monitored and recording should preferably be digital and be retained for a minimum of 30 days.
- Where applicable, register systems with the local law enforcement.

Digital Recording of Closed-Circuit Television

Digital recording of closed-circuit television cameras is recommended and should meet the specification details established by the Chief of Security. Specific requirements will depend on the type of digital recorder installed, the cost appraisal for the number of cameras to be recorded on opening, and the number of cameras likely to be used in the future. The Chief of Security shall control the digital recording system.

<u>Automated Access Control Systems</u>

Access to government facilities is controlled to ensure that only authorized persons gain access. At a minimum, access to facilities is controlled by a receptionist or card-access control system. Identify specific access requirements in the Security Policy and Procedure Manual.

The access control system should, at a minimum, incorporate electronic access control, alarm reporting, image capture, and badge production in conjunction with physical locks and key control to control access to the facility. The system shall be capable of providing

alarm output ”triggers” to the closed-circuit television system to allow camera scene of alarm areas to be displayed on the spot monitors in the Command and Control Center.

Facility Access Control

For the facility access control to be effective, the number of external access and egress points must be kept to a minimum but meet the requirements for fire safety. All regular access and egress points must be access controlled and have an anti-pass backup capability, which prevents a person from re-entering a secure area unless they follow the appropriate path. Remote operation of external doors must only be installed where they open into a secondary secure area which is viewed directly or by closed-circuit television. Internal doors providing access to primary and secondary critical areas should be controlled by electronic access control. Apply anti-pass back capabilities to all external doors where access control is necessary.

Security Officers and Patrols

Where applicable, security force officer level requirements is the decision of the Chief of Security and is based on an informed opinion from local, country, and government threats, specific vulnerabilities, identified risks, and their likelihood of occurring or being exploited.

Fully integrate security measures into one security control center. The security control center should provide the maximum protection to the security and reception staff and the systems data and information contained within.

Patrol Frequencies

At facilities with security force, reduce routine patrols to an initial patrol at the beginning of shift and a patrol to be conducted at the end of shift. It should, however, be emphasized that patrol frequencies are at the discretion of the local Security Captain. Patrol frequencies outside of normal working hours should be conducted at least four times during an eight-hour period on large sites. Smaller sites should be subjected to at least six patrols during an eight-hour period. Where sites are manned by a single security force officer, consideration should be given to waiving the requirement for patrols in favor of continual monitoring of closed-circuit television and alarm systems. If this practice is adopted, consider using internal intruder detection systems.

Lock and Key Controls

Keys can be easily copied from an impression or a photograph. Unauthorized persons are not to be given the opportunity to handle or examine security keys. There is a need for the strict control of keys. The policy regarding the issue, possession, and storage of keys is vital. The deciding factors in that policy should be necessity and accountability.

The following needs to be considered:

- Issue keys in accordance with the authorized employee and contractor identification system.
- Keep the number of keys issued for any lock to the minimum.

- Maintain a record (master key register developed by the local security force) showing the following:
  1. The date the working key (but not the duplicates) was signed out to the custodian
  2. The identifying features of each key such as the type registered, key number, and number of the duplicate
  3. The identifying details of persons allowed access to each key
- Check the keys in at the end of each working day when used to directly protect sensitive environments. Secure the keys, when not in use, in strong key boxes within the security control center.
- Ensure that keys are not accessible to persons who do not have authorized access to the material or to the room or area that the lock protects.
- Do not remove security keys from the facility without the specific authority of the Chief of Security.
- Treat in-use security keys at the same value and sensitivity as the material and environment they protect; store, protect, and handle the keys accordingly.
- Conduct periodic checks to account for all keys.
- Change keys and combinations when any of the following events occur:
  1. Loss or compromise of keys
  2. Suspected loss or compromise of keys
  3. Termination of employment of any key holder
  4. On a regular basis (every six months)

Spare Keys

The following conditions apply to spare keys:

- Hold spare keys to security locks centrally in approved security containers by a designated member of staff.
- Do not store spare keys in the same container as the working key.
- Issue a spare key only to persons with authorized access to the area or material the lock protects and only with documentation proving that the working key has been misplaced or lost.
- Record the details of the issued spare keys.
- Supply additional keys only on the written authority of Chief of Security.

Identification

Label the keys to facilitate their daily issue. Code the labeling in a way that does not readily identify the gate, door, or container to which the keys give access.
Check key rings frequently to ensure that keys cannot become detached.

<u>Entry Control Areas</u>

Basic minimum requirements for entry into a government facility include:

- Visitors must ask the person they are visiting to arrange access to the facility. The staff member must send an email to the security control center or reception desk informing them of their visitor's arrival at least 24 hours in advance.
- Issue all personnel a government identification card that must be visibly worn while on the facility. Revoke access rights to work areas immediately for any member of staff

who leaves the facility.
- Visitors to government facilities must obtain a visitor card at the reception desk and be accompanied at all times by an authorized person. Employees must challenge unaccompanied strangers or anyone not wearing a government identification card or pass in the workplace.
- Visitors to government facilities may be required to obtain permission prior to the day of the visit. Grant access only for specific purposes.
- Verify and authorize access by any external support services personnel.

Secure Asset Locations

Restricted spaces are typically located in the interior of the facility away from exterior windows, if practical. Floor plans for general use should not contain the location of critical assets. In general, construction of the restricted space will be slab-to-slab and adhere to government construction requirements.

If feasible, secure asset areas should not have glass doors or windows. Metal-clad doors or solid wood doors should be used at all restricted space entrances. Entrance to the secure asset areas will be via electronic access control with the capability of providing an audit trail. For exterior room doors having key access, hardware will be removed from the master key system of the facility. The issuance of non-master keys must be controlled and given only to individuals with an ongoing business need. Install an intruder detection system on all secure asset locations. The access control and intruder detection systems will have uninterrupted power supply backup.

Personnel Security Requirements

Only personnel having an ongoing recurring business need will be given unescorted access to the secure asset areas. If access is no longer required, the individual's name should be removed from the card access system. Visitors should be kept to a minimum, with tours conducted by authorized government personnel.

Summary

This baseline physical security measures instruction is the first step in assessing the types of security measures that could be applied to government facilities. The physical protection system report is used to evaluate the effectiveness of on-site security measures and to identify the need to provide additional measures or upgrade existing systems.

1.4 Develop Questions for Each Critical Infrastructure Component

Before conducting the site visit, you want to be sure to gather as much information as you can about critical infrastructure components. Recall that the components of critical infrastructure include: physical conditions, facility operations, facility policies and procedures, regulatory requirements, and safety and legal considerations.

Directions:

1. Prepare four questions for each of the critical infrastructure components listed in the sections that follow. Your questions can be similar to the sample questions that are provided for guidance. However, questions should be specific to the information provided for this facility.
2. Write your questions in the spaces provided.
3. Your team will have 15 minutes to write the questions.
4. Be prepared to conduct a report out (briefing) of your responses to the class.

Physical Conditions

Sample questions:

1. Has any building on the facility been threatened by a natural disaster or terrorist attack?
2. Has the topography or vegetation in the area prevented the security systems from working as they should?
3. Does the location of the facility allow easy access to outsiders such as the public?
4. Is the facility layout as depicted in the maps and drawings still accurate?
5. Are structures on the site still depicted accurately on the facility drawings?
6. Are infrastructure details such as ventilation and air conditioning, communications and information systems, location of hazardous materials available for review?

Facility Operations

Sample questions:

1. What is the mission of the facility and how does the critical infrastructure contribute to the mission?
2. Does the schedule of work activities reflect what was received during the data call?
3. Does the security force know and understand their guiding policies and procedures?
4. What is the work schedule of those involved with the facility operation? Your response should include open and closed periods, weekends, and holidays?
5. What are the security clearance requirements of employees? What are their respective job descriptions?
6. Are visitors allowed in the facility and if so, how is access controlled?

Facility Policies and Procedures

Sample questions:

1. What are the security requirements for security force personnel at the facility?
2. When was the last time, the security force conducted a performance test. If conducted, what were the results?
3. Can you show me the reports on violations of policies and procedures?
4. Are security systems performance tested, if so, when was the last test and what were the results?
5. Are the security systems performing as designed? As an example, do the sensors operate properly, does the closed circuit television view truly indicate who or what is in a specified area, and lastly are the physical barriers to the facility adequate?

Regulatory Requirements

Sample questions:

1. Who is the regulating authority for this facility, and is there more than one?
2. When was the last regulatory audit? What were the results?
3. What has the facility done to comply with regulations and findings by the authority?
4. Are there regulatory requirements for the facility's security force?

Safety Considerations

Sample questions:

1. When was the last safety inspection conducted of the facility area(s)?
2. Does the inspection include life safety issues such as confined space reviews (ensuring people are able to safely work in and escape from spaces that have limited access)?
3. Who responds to emergency situations such as fire and medical issues?
4. When was the emergency response plan last tested? What were the results?
5. Is there an evacuation plan? Has it been exercised?

Legal Considerations

Sample questions:

1. Are there any legal constraints on the facility and how it operates? If so what are they and how do they affect security operations?
2. Are there any current legal issues at the facility? If so, what are they?
3. What are the legal regulations that govern the security force's actions against a terrorist?
4. What are the past legal issues affecting the facility's operations?

This Page Intentionally Left Blank.

PART 2: CRITICAL INFRASTRUCTURE ASSETS (MODULE 6)

Purpose:	To prioritize consequences for a given critical infrastructure
Reference:	Module 6: Critical Infrastructure Assets
Duration:	110 minutes (90-exercise; 20-debrief)
Group composition:	Table groups
Debrief:	Presentation and discussion
Equipment:	National Ministries Building Complex Map

2.1: Identify Critical Infrastructure Assets and Loss Analysis

In *Module 5: Critical Infrastructure Components*, you participated in the first part of the National Ministries Building Threaded Exercise by forming teams and initiating a data call to the National Ministries Building facility director. Recall that information received back from the facility director included:

- A letter from the facility director describing characteristics of the building
- Maps
- Floor plans
- Regulations regarding physical security policies and procedures

The facility director did not provide specific information regarding critical assets; instead, the director stated, "I am not sure what is meant by 'critical asset' area, but all areas receive the same consideration for safety."

Due to the missing information regarding critical assets, your vulnerability analysis team should have requested additional information from the facility director regarding the National Ministries Building's critical assets. For now, assume the additional information has been requested, and the response was provided in a second letter from the National Ministries Building Facility Director (refer to Facility Director's Second Response Letter). Your team will use this information and the information you have collected up to this point to conduct an **undesirable consequences of critical asset loss analysis**.

Directions:

1. Review and discuss the Facility Director's Second Response Letter, below, with your team.
2. Use the information presented in the letter to work with your team members to identify critical assets belonging to the National Ministries Building.
3. Use all the information that you have received and compiled to this point to complete *Table 2: Undesirable Consequences of Critical Asset Loss Analysis*.
   - Column 1: write the critical assets you identified in the facility director's letter
   - Columns 2 and 3: assume that all undesirable consequences of critical asset loss are related specifically to the identified critical asset

- Column 4: apply your team's best collective judgment (based on personal knowledge or professional expertise) to determine probability of occurrence levels

This Page Intentionally Left Blank.

Facility Director's Second Response Letter

From: Facility Director
National Ministries Building
National Avenue
Capital City

To: Vulnerability Analysis Team

In response to your request for additional data on the types of assets we have at the National Ministries Building, I hope the following information meets your requirements.

People:
Highest population level is about 1000, typically observed Monday through Friday during normal work hours. The Head of State, her staff, and eight ministers and their staffs are housed in the National Ministries Building and all are considered extremely important to the daily functions of the country's government. The ministers' staff are scattered throughout the building, usually in their assigned areas. A wide variety of visitors come each day to the building and include visitors to each minister, the Head of State, and dozens of people to the National Museum.

Information:
Each minister possesses important information about his or her operations and most is restricted data, only for those who have a need to know. The information is not for public dissemination. The Ministry of Interior has extremely important intelligence information that should never be disseminated without several approval levels. Each ministry has a room that contains his or her information with only personnel who work in the area allowed in the room. The Ministry of Interior is the largest office in the building and needs to secure information at a higher level due to its level of importance.

Processes:

The Ministries of Interior, Justice, and Taxation have processes that must be protected. The Ministry of Justice is responsible for checking criminal data and dissemination, as required. There is a country requirement that all information is disseminated in a timely manner and such responses must be flawless.

The Ministry of Interior is responsible for the collection, analysis, and dissemination of intelligence products. Failure to accomplish any of these processes would have a critical effect on the country's ability to protect its citizens.

The Ministry of Taxation is responsible for sending out all tax notices, collection of monies, and sending tax refunds back to citizens. The collection of taxes is extremely important to the country's ability to operate on a daily basis. The refund process, although important, does not have the same level of requirement.

All the ministers believe that it is extremely important that they have the ability to always communicate to their staff in other buildings, provide information to the country's citizens through the media, and be available for people to come to the National Ministries Building to interact with their government officials.

Equipment:
The National Museum contains over 100 pieces of art, with an additional 50 irreplaceable artifacts. In addition to the monetary value of each item, most are considered icons for our country and it is felt by senior government officials that all are priceless.

Computers are an integral part of the government's ability to operate. Processing computers and related equipment for the Ministry of Interior, Ministry of Justice, and Ministry of Taxation are critical for the government's ability to operate and provide security. Although each ministry has computers, most do not maintain the important for-official-use-only designation. Those that do are stored in the rooms containing such information.

Should you need additional information, please let me know.

Respectfully,

Charles J. Lewis

Facility Director
National Ministries Building

Table 2: Undesirable Consequences of Critical Asset Loss Analysis

Critical Infrastructure: Venue Facility — National Ministries Building			
Column 1 **Critical Asset**	**Column 2** **Undesirable Consequences of Critical Asset Loss**	**Column 3** **Levels of Undesirable Consequences of Critical Asset Loss**	**Column 4** **Probability of Occurrence of Undesirable Events**
People:			
Information:			

Critical Infrastructure: Venue Facility — National Ministries Building			
Column 1 **Critical Asset**	**Column 2** **Undesirable Consequences of Critical Asset Loss**	**Column 3** **Levels of Undesirable Consequences of Critical Asset Loss**	**Column 4** **Probability of Occurrence of Undesirable Events**
Processes:			
Equipment:			

2.2: Create Threat Spectrum Matrix

Directions:

1. Discuss and complete Table 3: Threat Spectrum Matrix — National Ministries Building with your team.
2. Transfer information from Table 2 into the appropriate cells within the threat spectrum matrix.
3. Recall that you may have several asset-related consequences of loss within any one given cell.
4. Your team will have 30 minutes to complete this exercise.
5. Be prepared to share your completed threat spectrum matrix with the class.

Table 3: Threat Spectrum Matrix — National Ministries Building

Facility: National Ministries Building			
High Consequence			
Medium Consequence			
Low Consequence			
	Low Probability	**Medium Probability**	**High Probability**

This Page Intentionally Left Blank.

PART 3: THREAT ANALYSIS (MODULE 10)

Purpose: To prepare a threat analysis statement
Reference: Module 10: Analyzing the Threat
Duration: 60 minutes (45-exercise; 15-debrief)
Group composition: Table groups
Debrief: Team presentation
Equipment: National Ministries Building Complex Map

3.1 Prepare the Threat Analysis

In this part of the exercise, you will continue working with your vulnerability analysis team to examine existing adversarial threats (both insiders and outsiders) and estimate the likelihood of attack. Based on that analysis, you will develop a threat analysis statement that creates the foundation for subsequent security countermeasure evaluation and improvement.

Remember 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. The analysis is based on best analysis derived from the information received. Your team must ensure they are analyzing facts and not making decisions based on opinion. The data has to support the conclusion.

Two teams will complete the worksheet for the Insider Threat, while the remaining two teams will complete the Outsider Threat worksheet. You have 45 minutes to complete the assigned worksheet and write the threat analysis statement. Be prepared to discuss your responses and rationale for each rating.

Directions:

1. Read the section titled National Ministries Building Data Collection and identify all insider and outsider threat related information.
2. If assigned, complete Table 4: Insider Threat Information Worksheet by assigning the appropriate rating (high, medium, or low) to each insider threat your team identifies.
3. If assigned, complete Table 5: Outsider Threat Information Worksheet.
   - Begin this part of the threat analysis by examining the information you collected about any outsider threats.
   - Note that Table 5 indicates that there are two outsider threats.
   - To complete this worksheet, your team must select at least two primary threats to analyze and rate the elements for each category listed.
4. Complete Table 6: Estimating Likelihood of Attack Worksheet (1) and Table 7: Estimating Likelihood of Attack Worksheet (2).

- Refer to information from completed table from your worksheet as well as the information contained in the section titled National Ministries Building Data Collection.
- Discuss the estimated likelihood of attack and document your responses in Tables 6 and 7.
- The Estimating Likelihood of Attack Worksheet uses a numerical scoring range of 1 to 10, with a "10" determined to be the most critical.
- You may decide to change the listed values for each category, but you should seriously consider and justify any modification to meet the specific requirements.

5. After you complete these tasks, discuss and prepare your threat analysis statements. Be sure to write a separate threat analysis statement for each threat.
6. Document your threat analysis statements in the space provided in **3.3 Threat Analysis Statements**.
   - Remember that the threat analysis statement is a written description of the results of the tables you completed.
   - The team should focus on those threats that provide the highest level of risk and describe in as much detail as possible the attributes of the adversaries involved.
7. Your team will have 45 minutes to complete this exercise.
8. Be prepared to share your responses with the class.

3.2 National Ministries Building Data Collection

National Ministries Building
Data Collection
Prepared by the Office of Security
For the Vulnerability Analysis Team

Intelligence Report: Urban Front Terrorist Organization

This group has been known to operate in cells to commit acts of violence throughout adjacent countries. Their primary tactic is and has continued to be vehicle and suicide bombs. They typically drive to a facility, park a large panel truck near the entrance of the facility, and abandon the vehicle. Once people gather at the facility, the terrorists detonate the bomb with a remote device. Their primary motivation is to cause discontentment among the citizens by having them believe the government is powerless in stopping the attacks.

At least five people have been identified as part of this group, but there were others that have died as a result of their involvement in suicide bombings. The group's suicide bomb tactics focus on gatherings of people who are attending national symbols such as museums, monuments, and government buildings.

The suicide bombers have killed dozens of people over the past three months. In each of the incidents, the sequence of events is essentially the same: the suicide bombers encounter the local authorities before entering the building, and then the device explodes. Witnesses report that in each incident, the bombers never touched or triggered the device, which suggests that the suicide bombers are being detonated remotely.

Union Brochure

An intelligence source discovered a union brochure that discussed an upcoming strike against the government. The "Workers United for a Better Life" Union announced in the brochure that it would conduct a planned strike very soon. The brochure did not give a specific date. The organization represents 1,000 government employees who have been disgruntled for the past three years due to poor pay and no salary increases.

The brochure also said that the employees will leave their offices at the appointed hour and go to the National Ministries Building and establish a human chain around the building, preventing anyone from entering or leaving. If necessary, anyone desiring to break the chain will be dealt with by the use of a "pepper spray" irritant. Protestors are instructed to wear masks during the protest.

The government has avoided such protests in the past through quick negotiations, but the Union has never made an effort of this type. Recently appointed union leadership is known for its radical behavior at past events, but has never been able to get people organized enough to carry out this type of threat.

Excerpts from the Head of Government's Newsletter

Dear Civil Servants,

It is with extreme dismay that I must announce the layoff of 500 government employees due to budget concerns. I have met with each of the Ministers to discuss the best way to deal with this situation, and it has been determined that employees holding critical positions will remain working in the primary offices of each Ministry.

Since I cannot tell you when or if you will be coming back to work for the government, arrangements have been made to help you transition to other positions in the private sector. The names of those affected will be announced next week.

Adjacent Country Intelligence Report

A suicide bomber entered the Museum of History recently and went directly to the cafeteria, where the staff and faculty were meeting with the Minister of Antiquities. Once inside the cafeteria area the bomber detonated the bomb, which resulted in 10 people being killed and dozens injured.

A call was received shortly after the incident from a male individual claiming to be a member of the Urban Front terrorist organization. The bomber was identified as an employee of the Museum.

Media Report

The National newspaper reported, "Police are investigating a serious security breach after a civil servant lost top-secret documents containing the latest intelligence on Urban Front."

The unnamed Ministry of Interior employee apparently breached strict security rules when he left the papers on the seat of a train. Another passenger spotted the envelope with the files and gave it to the National newspaper who gave them to the police. The employee was later suspended from his job, the Ministry Office said.

The Head of Government is being asked to conduct an extensive review of policies related to classified documents. Some members of Parliament are asking for the Head of Government to step down and take full responsibility for the actions of employees under her charge.

Table 4: Insider Threat Information Worksheet

Threat opportunity → / Insider categories ↓	Access to asset	Access to physical protection system	Knowledge of security	Theft opportunity	Sabotage opportunity	Conspiring opportunity

Table 5: Outsider Threat Information Worksheet

Threat Type	Threat 1	Threat 2
Potential Action (High, Medium, Low)		
Theft		
Sabotage		
Other:		
Motivations (High, Medium, Low)		
Political		
Philosophical		
Social		
Economic		
Personal		
Other:		
Tactics		
Stealth Force Deceit		
Capabilities		
Number		
Technical expertise		
Insider assistance		
Weapons		
Equipment or tools		
Transportation		

Threat Type	Threat 1	Threat 2
Other:		

Table 6: Estimating Likelihood of Attack (L_A) Worksheet (1)

Estimating Likelihood of Attack (L_A) Worksheet				
Date: XX/XX/20XX			Recorded by:	
Facility identifier:				
Threat type:				
Capability:				
Is the adversary group capable of conducting a successful attack on this facility? To answer the question, consider: Is the adversary group: Located near or able to gain access to the facility? Expected to have the material resources to attack this facility? Expected to have the technical skills to attack this facility? Expected to have the planning and organizational skills to attack this facility?			**If Yes, continue**	**If No, L_A = very low, Stop**
Instructions for the following section: Select the answer from the three middle columns that most accurately describes the item contained in the **Category** column of each row. Note the numeric value associated with that answer and enter the numeric value in the **Score** column.				
History and Intent:				**Score**
Category: Historical Interest	If there is documented evidence that historically, this adversary group has shown interest in this type of facility or this specific facility Score = 5	If there is speculation but no evidence that this adversary group has shown interest in this type of facility or this specific facility Score = 3	If there is no evidence that this adversary group has ever shown interest in this type of facility or this specific facility Score = 1	**Score =**

Estimating Likelihood of Attack (L_A) Worksheet				
Category: Historical Attacks	If there is documented evidence that historically, this adversary group has conducted similar attacks at this type of facility or this specific facility Score = 5	If there is speculation but no evidence that this adversary group has conducted similar attacks at this type of facility or this specific facility Score = 3	If there is no evidence that this adversary group has conducted similar attacks at this type of facility or this specific facility Score = 1	**Score =**
Category: Current Interest In Facility	If current information suggests interest in the facility Score = 10	Not applicable	If there is no current information that suggest interest in the facility Score = 2	**Score =**
Category: Current Surveillance	If current intelligence verifies surveillance at the specific site Score = 10	If current intelligence verifies surveillance at other similar facilities in the country or abroad Score = 6	If current intelligence does not involve the specific facility, in the country, or abroad Score = 2	**Score =**

Estimating Likelihood of Attack (L_A) Worksheet				
Category: Documented Threats	If this site has received documented threats of attack by this type of threat Score = 10	If this site has received documented threats of attack, but not of this threat type Score = 6	If this site has not received documented threats from this threat type or other adversary groups Score = 2	**Score =**
Relative Attractiveness of Target				**Score**
Category: Consequence	If level of estimated consequence for attack is consistent with goals of this threat type Score = 10	If level of estimated consequence caused by attack is not definitely consistent with goals of this threat type but possibility exists Score = 6	If level of consequence caused by attack is not at all consistent with goals of this threat type Score = 2	**Score =**
Category: Ideology	If attacking this site is consistent with ideology or motivations of this threat type Score = 10	If attacking this site is not consistent with ideology or motivations of this threat type, but the possibility exists Score = 6	If attacking this site is not at all consistent with the ideology or motivations of this adversary group Score = 2	**Score =**

Estimating Likelihood of Attack (L_A) Worksheet				
Category: Ease of Attack	If perception exists that physical protection system is relatively easy to defeat or does not exist, or the undesired event is easily accomplished at this site Score = 5	If perception exists that physical protection system provides moderate protection, or there is moderate difficulty in accomplishing the undesired event at this site Score = 3	If the perception exists that the site has a robust, effective physical protection system or the undesired event is extremely difficult to accomplish at this site Score = 1	**Score =**
Total Score for Threat Type				**Total**
Write the total of all above scores in this box ➔				
Likelihood of this Threat Type attacking this facility — L_A				
If the total score for this threat type is: ≥ 60, L_A = Very High ≤ 59 and ≥ 47, L_A = High ≤ 46 and ≥ 32, L_A = Medium ≤ 31 and ≥ 19, L_A = Low ≤ 18, L_A = Very Low Write threat level based on L_A score➔				

Notes:

Table 7: Estimating Likelihood of Attack (L_A) Worksheet (2)

Estimating Likelihood of Attack (L_A) Worksheet				
Date: XX/XX/20XX			Recorded by:	
Facility identifier:				
Threat type:				
Capability:				
Is the adversary group capable of conducting a successful attack on this facility? To answer the question, consider: Is the adversary group: Located near or able to gain access to the facility? Expected to have the material resources to attack this facility? Expected to have the technical skills to attack this facility? Expected to have the planning and organizational skills to attack this facility?			**If Yes, continue** ☐	**If No, L_A = very low, Stop**
Instructions for the following section: Select the answer from the three middle columns that most accurately describes the item contained in the **Category** column of each row. Note the numeric value associated with that answer and enter the numeric value in the **Score** column.				
History and Intent:				**Score**
Category: Historical Interest	If there is documented evidence that historically, this adversary group has shown interest in this type of facility or this specific facility Score = 5	If there is speculation but no evidence that this adversary group has shown interest in this type of facility or this specific facility Score = 3	If there is no evidence that this adversary group has ever shown interest in this type of facility or this specific facility Score = 1	**Score =** ☐

Estimating Likelihood of Attack (L_A) Worksheet				
Category: Historical Attacks	If there is documented evidence that historically, this adversary group has conducted similar attacks at this type of facility or this specific facility Score = 5	If there is speculation but no evidence that this adversary group has conducted similar attacks at this type of facility or this specific facility Score = 3	If there is no evidence that this adversary group has conducted similar attacks at this type of facility or this specific facility Score = 1	**Score =**
Category: Current Interest In Facility	If current information suggests interest in the facility Score = 10	Not applicable	If there is no current information that suggest interest in the facility Score = 2	**Score =**
Category: Current Surveillance	If current intelligence verifies surveillance at the specific site Score = 10	If current intelligence verifies surveillance at other similar facilities in the country or abroad Score = 6	If current intelligence does not involve the specific facility, in the country, or abroad Score = 2	**Score =**

Estimating Likelihood of Attack (L_A) Worksheet				
Category: Documented Threats	If this site has received documented threats of attack by this type of threat Score = 10	If this site has received documented threats of attack, but not of this threat type Score = 6	If this site has not received documented threats from this threat type or other adversary groups Score = 2	**Score =**
Relative Attractiveness of Target				**Score**
Category: Consequence	If level of estimated consequence for attack is consistent with goals of this threat type Score = 10	If level of estimated consequence caused by attack is not definitely consistent with goals of this threat type but possibility exists Score = 6	If level of consequence caused by attack is not at all consistent with goals of this threat type Score = 2	**Score =**
Category: Ideology	If attacking this site is consistent with ideology or motivations of this threat type Score = 10	If attacking this site is not consistent with ideology or motivations of this threat type, but the possibility exists Score = 6	If attacking this site is not at all consistent with the ideology or motivations of this adversary group Score = 2	**Score =**

Estimating Likelihood of Attack (L_A) Worksheet				
Category: Ease of Attack	If perception exists that physical protection system is relatively easy to defeat or does not exist, or the undesired event is easily accomplished at this site Score = 5	If perception exists that physical protection system provides moderate protection, or there is moderate difficulty in accomplishing the undesired event at this site Score = 3	If the perception exists that the site has a robust, effective physical protection system or the undesired event is extremely difficult to accomplish at this site Score = 1	**Score =**
Total Score for Threat Type				**Total**
Write the total of all above scores in this box ➔				
Likelihood of this Threat Type attacking this facility — L_A				
If the total score for this threat type is: ≥ 60, L_A = Very High ≤ 59 and ≥ 47, L_A = High ≤ 46 and ≥ 32, L_A = Medium ≤ 31 and ≥ 19, L_A = Low ≤ 18, L_A = Very Low Write threat level based on L_A score➔				

Notes:

3.3 Threat Analysis Statements

Threat 1:

Threat Analysis Statement for:

Threat 2:

Threat Analysis Statement for:

PART 4: BOMB THREAT MANAGEMENT POLICY (MODULE 11)

Purpose:	To create a bomb threat management policy for the National Ministries Building by answering a series of questions
Reference:	Module 11: Policies and Procedures
Duration:	30 minutes (20-exercise; 10-debrief)
Group composition:	Table groups
Debrief:	Large-group discussion
Equipment:	National Ministries Building Complex Map

Directions:

1. Work with your table group to fill in the missing information in *Table 8: Bomb Threat Management Plan Considerations*.
2. Discuss with your group the possible bomb threat management considerations for each question in the **Question** column and record your responses in the **Considerations** column; for example, the first question in the **Question** column states, "Identify who should be responsible for both policy and incident command." Discuss this question with your team members and document your response in the **Considerations** column.
3. While you may not be able to develop a complete bomb threat management policy for the National Ministries Building, your group will have a good start on the various elements to include in such a policy once you have completed Table 8.
4. Refer back to the policies and procedures outlined previously in this module.
5. Your team will have 20 minutes to complete this exercise.
6. Be prepared to share your answers with the class.

Table 8: Bomb Threat Management Plan Considerations

Questions	Considerations
Identify who should be responsible for both policy and incident command.	
Who should be designated as floor wardens?	
What are some strategies you could implement to ensure that the National Ministries Building employees know what to do if they receive a bomb threat?	
If an employee at the National Ministries Building receives a bomb threat, what is the most important information the recipient of the threat should attempt to obtain from the caller?	
What characteristics might indicate the authenticity of a caller's threat?	
Identify a location for the incident command post under both nonevacuation and evacuation response conditions.	

Questions	Considerations
What are the three primary methods you could use for search and evacuation in response to a bomb threat? State one advantage and one disadvantage for each.	
If a suspicious device is discovered, what elements should the incident commander be prepared to discuss with local authorities?	

This Page Intentionally Left Blank.

PART 5: SECURITY FORCE OPERATIONS (MODULE 12)

Purpose: To develop a security force response plan
Reference: Module 12: Security Force Operations
Duration: 60 minutes (30-exercise; 20-presentations; 10-debrief)
Group composition: Table groups
Debrief: Team presentation; facilitator feedback
Equipment: National Ministries Building Complex Map

Directions:

1. Refer back to the National Ministries Building Data Collection section in **Part 3: Threat Analysis**. Use this information to develop your response plan for the planned strike by the Workers United for a Better Life.
2. Use *Table 9: Protest and Demonstration Response Plan Applicability* to document your response plan. As you develop your plan, you may use any existing plan(s) available in your agency to complete the references section of the plan.
3. Use your team's collective judgment (based on personal knowledge or professional expertise) when completing Table 9.
4. Your team will have 30 minutes to complete this exercise.
5. Be prepared to discuss your team's security force response plan and explain the rationale use for solutions derived to the class.

Table 9: Protest and Demonstration Response Plan Applicability

Protest and Demonstration Response Plan Applicability: Protective Force Members Date: _____
References: Identify the types of references that would be applicable. Provide the title of other documents that relate to the plan; for example, a plan on bomb threats may reference the building evacuation plan for a specific location.
Definitions and Abbreviations: Identify such terms as **protester** or **demonstrator**; use this section as a quick reference for identified terms or for abbreviations used in the plan.
Purpose: Why is this response plan important? This section covers the specific area the plan was developed to address and personnel affected by the plan.

Protest and Demonstration Response Plan **Applicability: Protective Force Members** **Date: _____**
Guidance: What are security force members expected to do during the protest or demonstration? Provide the response plan users with the steps for what to do in the event the plan is to be implemented—areas to consider may be existing policies and procedures, protection strategies, tactical response options, actions, times, location, access to asset, chain of command, outside resources, communication, and event logs for future reference and training.
Reporting: What are security force members expected to do after the protest or demonstration terminates? Identify the post-event reporting requirements should the plan require implementation.

PART 6: SECURITY TECHNOLOGY (MODULE 13)

Purpose:	To develop a security technology plan for the protection of the National Ministries Building
Reference:	Module 13: Security Technology
Duration:	60 minutes (40-exercise; 20-debrief)
Group composition:	Table groups
Debrief:	Presentation and discussion
Equipment:	National Ministries Building Complex Map

Develop a Security Technology Plan

You will now work with your team to develop a technology plan for the National Ministries Building. Before you begin, review Adjacent Country Intelligence Report and Related Threat Analysis Statements. This information has already been provided to you in the section from *Module 10: Analyzing the Threat*, entitled National Ministries Building Data Collection in Part 3: Threat Analysis.

As you develop your technology plan, base your team's conclusions on the following:

- The Adjacent Country Intelligence Report and Related Threat Analysis Statements
- Letter from National Ministries Building Facility Director in Response to Data Call (recall that this information was provided to you in the Facility Director's Second Response Letter, found in Part 2: Prioritizing Critical Assets)

As you develop your plans, recommend any detection and assessment, delay, and response solutions that appear to effectively prevent or mitigate the threat. Also, note that while the focus is on technical solutions, you can also recommend nontechnical solutions and related security and protection policies and procedures.

Directions:

1. Refer back to the section titled National Ministries Building Data Collection in **Part 3: Threat Analysis** in *Module 10: Analyzing the Threat*. Pay particular attention to the Adjacent Country Intelligence Report.
2. Read through the finalized threat analysis statements for the Urban Front Terrorist organization and Union Workers for a Better Life activist group and the Intelligence Bulletin below.
3. Develop a technology plan for the National Ministries Building. Base your plan on:
    - The Adjacent Country Intelligence Report, Related Threat Analysis Statements, and the Intelligence Bulletin.
    - Letter from National Ministries Building Facility Director in Response to Data Call (recall that this information was provided to you in the Facility Director's Second Response Letter, found in Part 2: Prioritizing Critical Assets)
4. Document your team's solutions in *Table 10: Security Technology Plan for National Ministries Building*. Make sure your team's plan addresses all functions of an effective physical protection system: detection and assessment, delay, and response.
5. Your team will have 1 hour to complete the worksheet.

Finalized Threat Analysis Statements and Intelligence Bulletin

Finalized Threat Analysis Statement for
Urban Front Terrorist Organization

It is believed that the Urban Front Terrorist organization may attempt to detonate an explosive device outside a national icon through the use of a vehicle bomb near the facility or through the use of a suicide bomber inside a national icon. The terrorist's desire would be to create a mass casualty situation. The use of an insider is highly probable based on similar attacks in adjacent countries. The use of a remote detonation device is highly probable. Based on a score of 36, with no current targeting information related to the National Ministries Building to either increase or decrease the score, it is believed that an attack on the National Ministries Building by this group is rated as medium probability.

Finalized Threat Analysis Statement for
Union of Workers for a Better Life Activist Group

It is believed that the Union of Workers for a Better Life has targeted the National Ministries Building for a future protest. The number of protestors is estimated at one hundred, but could exceed that number considering that the group's total membership is estimated to be over 1000 members. Although not known to be highly organized in the past, due to recent elections the group may begin to develop serious activist tactics. Intelligence gathered on the new leader of the group found he is encouraging the use of pepper spray on noncompliant members and public safety authorities. Due to layoffs of employees, tensions at the protest will be extremely high and potentially volatile. Based on a score of 52, there is a high probability that the Union will conduct protests at the National Ministries Building.

Intelligence Bulletin concerning

Union of Workers for a Better Life Activist Group

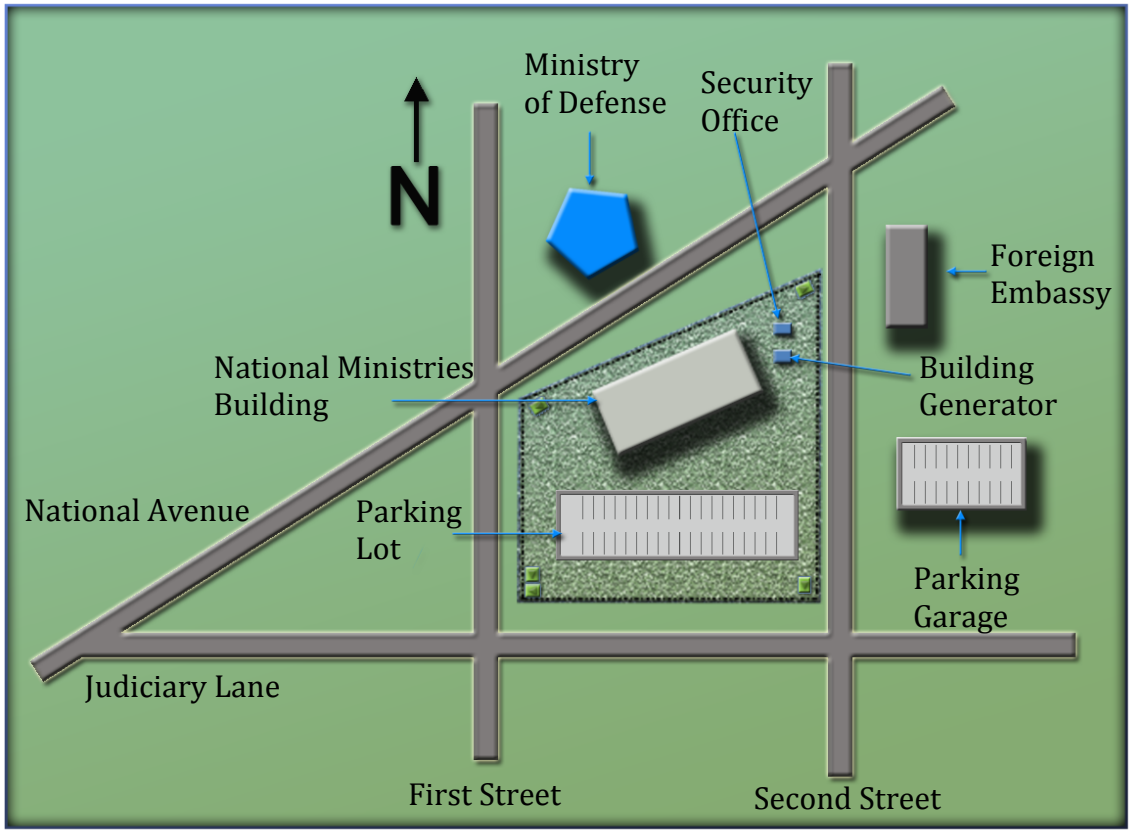
Verified law enforcement intelligence reports confirm that a laid off information technology group leader has developed a software program that is capable of overcoming the intrusion detection system of the National Ministries Building computer system. Recent law enforcement database entries indicate two intrusions in the last two weeks using techniques similar to the capabilities of this software program. No data or information was corrupted. These appear to be test or rehearsal intrusions for a future attack. Because of the upcoming protest, the possibility that the National Ministries Building computer system might experience an attack at the same time is highly likely.

Table 10: Security Technology Plan for National Ministries Building

Detection and Assessment
Delay

Response

National Ministries Building Complex Map



PART 7: SECURITY INSPECTION AND VALIDATION (MODULE 14)

Purpose:	To develop a security inspection and validation checklist for the National Ministries Building
Reference:	Module 14: Security Inspection and Validation
Duration:	60 minutes (45-exercise; 15-debrief)
Group composition:	Table groups
Debrief:	Large-group discussion
Equipment:	National Ministries Building Complex Map

Develop the Security Inspection and Validation Checklist

You will now work with your team to evaluate the effectiveness of the physical protection system for the National Ministries Building by discussing how to conduct a security inspection and validation for the National Ministries Building. Recall that an effective security inspection and validation program addresses three phases: inspection planning, conducting the inspection, and close-out.

Directions:

1. To complete Phase 1, your team must:
   - Discuss what should be accomplished in Phase 1 to prepare for conducting the actual security inspection.
   - Identify the essential action items that should be completed prior to conducting the security inspection and validation program. **Note:** You will not accomplish these actions during this exercise.
   - Document the action items in *Table 11: Security Inspection Planning for the National Ministries Building*.
2. To complete Phase 2, your team must:
   - Develop a security inspection and validation checklist that could be used during the security evaluation and inspection of the National Ministries Building.
   - Discuss the checklist questions that address security countermeasures for the National Ministries Building in the areas of policies and procedures, security force, and technology; technology includes intrusion detection systems and delay barriers.
   - Refer back to Facility Director's Response Letter and all provided information in **Part 1: Assessing Critical infrastructure Components** to develop your team's checklist. Record your checklist questions in *Table 12: Security and Inspection Validation Checklist for the National Ministries Building*.
   - Once the checklist is completed, go back and answer each question by selecting either **Yes** or **No** for each security countermeasure.
   - Be prepared to share your answers with the class.
3. To complete Phase 3, your team must:
   - Discuss what should be accomplished in Phase 3, once the inspection is complete.
   - Identify essential action items that should be completed after conducting the security inspection validation. Note: you will not accomplish these actions during this exercise.
   - Document the action items in *Table 13: Security Inspection and Validation for Close-Out for the National Ministries Building*.
4. Your team will have 45 minutes to complete this exercise.
5. Be prepared to share your answers with the class.

Table 11: Security Inspection Planning for the National Ministries Building

Phase 1: Inspection Planning
Prior to the actual security inspection validation of the National Ministries Building, what needs to be accomplished?

Table 12: Security Inspection and Validation Checklist for the National Ministries Building

Phase 2: Security Inspection and Validation		
Checklist Question	**Yes**	**No**
Policies and Procedures		
1.		
2.		
3.		
4.		
5.		
6.		

Phase 2: Security Inspection and Validation		
7.		
Security Force Personnel		
1.		
2.		
3.		
4.		
5.		
6.		
7.		
Technology: Intrusion Detection System		
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		

Phase 2: Security Inspection and Validation		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		

Phase 2: Security Inspection and Validation		
Technology: Delay Barriers		
1.		
2.		
3.		
4.		
5.		
6.		
7.		

Table 13: Security Inspection and Validation Close-Out for the National Ministries Building

Phase 3: Close-Out
After the actual security inspection and validation of the National Ministries Building, what needs to be accomplished?

PART 8: OPERATIONAL RESILIENCE PLAN (MODULE 15)

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
Equipment:	National Ministries Building Complex Map

Develop Operational Plan Security Countermeasure Recommendations

Performing Gap Analysis

Your team will now develop security countermeasure recommendations for the National Ministries Building as part of an operational resilience plan. To complete this part of the exercise, your team will have to refer back to the security inspection and validation checklist that you completed in **Part 7: Security Inspection and Validation,** *Module 14: Security Inspection and Validation,* and focus on those security countermeasures that will address the most significant vulnerabilities in the physical protection system. The identified vulnerabilities, recommended security countermeasures, and performance expectations for the solution your team is recommending will provide the basis for developing a resilience plan. In your own organizations, you would have completed a security inspection and validation report from the information contained in your security inspection and validation checklists.

When you perform a gap analysis in your own organization, three sections of the security inspection and validation report will provide the information you need.

- Performance test requirements
- Recommendations
- Conclusions

As you review your three choices from the checklist and discuss recommendations, your team can now clarify possible expected outcome requirements for the question areas and determine which collaborative groups would be appropriate to assist in the actions you are proposing. Because you are taking the examples and solutions from your unique security inspection and validation checklist generated in Module 14, there are no pre-determined answers to this activity.

Document your choices and recommendation in *Table 14: Integrating Security Inspection and Validation Results and Gap Analysis*. Be prepared to share one of your examples with the class.

Prioritizing Recommendations

To help your team clarify and prioritize the recommended actions you documented in *Table 14: Integrating Security Inspection and Validation Results and Gap Analysis*, you will complete *Table 15: Proposed Countermeasure Categories and Priorities*. Write your actions according to the countermeasure section.

- For example, in the fence sensor scenario, the recommendation to replace the fence section would be placed under the **Technology** section, while the recommendation to post a security force member at the nonfunctioning section should be placed under the **Security Force** section.
- Remember, one proposed action may have more than one entry, especially if it does not already have a policy and procedure in place or it involves several aspects of the same countermeasure.
- You may not have enough entries to fill out every line in the worksheet.

Once you have documented your recommendations, determine the priority of each line within each countermeasure section by checking if it is priority one, two, or three. Be prepared to share one of your examples with the class.

Directions:

1. Refer to the security inspection and validation checklist you completed in Part 7: Security Inspection and Validation (*Module 14: Security Inspection and Validation)*. Focus only on those items checked **No**, then select one item from each of the security countermeasures (Policies and Procedures, Security Force Personnel, Technology: Intrusion Detection System, and Technology: Delay Barriers) to be analyzed in *Table 14: Integrating Security Inspection and Validation Results and Gap Analysis*. This will be the link from your security inspection and validation to the resilience plan. Notice the **Results** column in *Table 14: Integrating Security Inspection and Validation Results and Gap Analysis* below was completed for you using the information from the **Addendum 15.1: Gap Analysis Process Scenario** that discussed a fence sensor. Use this information as an example to aid you in completing Table 14.
2. Complete Table 14 by referring back to the information in the security inspection and validation checklist. Be sure to complete all seven sections of Table 14 by entering the choices determined. The choices should be entered in order of preference (Choice #1, Choice #2, and Choice #3).
3. Complete *Table 15: Proposed Countermeasures Categories and Priorities* using the information from Table 14. Your team should transfer the information from Table 14 to the corresponding sections (Policies and Procedures, Security Force, and Technology) of Table 15.
4. After transferring the information from Table 14 to Table 15, select a priority level in which the proposed actions should be taken.
5. Record your team's security upgrade recommendations in the space provided.
6. Determine which recommendations should be included in the operational resilience plan because of their high priority and write those in *Table 16: Operational Resilience Plan Main Points* to address prevention, preparedness, response, and recovery in the plan.
7. Your team will have 40 minutes to complete the tables exercise and 5 minutes to present your results to the class.

This Page Intentionally Left Blank.

Table 14: Integrating Security Inspection and Validation Results and Gap Analysis

Results	Example:	Choice #1: Technology	Choice #2: Policies and Procedures	Choice #3: Security Force
1. Choice description	Fence sensors — Conclusion to replace the malfunctioning section of fence			
2. Expected standard requirements	100% Accuracy 0% false alarm rate 0% nuisance alarm rate Notes: Management requires 100% accuracy, so the assumption is that a 0% false alarm rate and 0% nuisance alarm rate are also desired.	___% Accuracy ___% false alarm rate ___% nuisance alarm rate Notes:		
3. Performance level results	☐ Satisfactory ☐ Marginal ☑ Unsatisfactory Notes: The fence performs correctly 0% of the time. This is unsatisfactory.	☐ Satisfactory ☐ Marginal ☐ Unsatisfactory Notes:	☐ Satisfactory ☐ Marginal ☐ Unsatisfactory Notes:	☐ Satisfactory ☐ Marginal ☐ Unsatisfactory Notes:

Results	Example:	Choice #1: Technology	Choice #2: Policies and Procedures	Choice #3: Security Force
4. Performance gap	100% non-performance			
5. Risk management	☐ No action ☐ Transfer issue ☑ Accept and mitigate Notes:	☐ No action ☐ Transfer issue ☐ Accept and mitigate Notes:	☐ No action ☐ Transfer issue ☐ Accept and mitigate Notes:	☐ No action ☐ Transfer issue ☐ Accept and mitigate Notes:
6. Proposed actions from security inspection and validation report	1. Management is posting a security force member at the fence section while the fence is non-functional. 2. The organization will replace the fence section.	1. 2.	1. 2.	1. 2.

Results	Example:	Choice #1: Technology	Choice #2: Policies and Procedures	Choice #3: Security Force
7. Collaborative groups	☑ Financial ☐ Human resources ☐ Information technology ☐ Legal ☐ Operational Area ☑ Security Operations Notes: Security Operations will be involved to schedule the interim security force member. Financial will be involved in the procurement process of the new section of fence.	☐ Financial ☐ Human resources ☐ Information technology ☐ Legal ☐ Operational Area ☐ Security Operations Notes:	☐ Financial ☐ Human resources ☐ Information technology ☐ Legal ☐ Operational Area ☐ Security Operations Notes:	☐ Financial ☐ Human resources ☐ Information technology ☐ Legal ☐ Operational Area ☐ Security Operations Notes:

This Page Intentionally Left Blank.

Table 15: Proposed Countermeasure Categories and Priorities

Write the options for proposed countermeasures in the **Category** column. In the **Priority Level** column, determine the priority for each countermeasure (low, medium, high).

Category	Priority Level
Technology	
	☐ Low ☐ Medium ☐ High
	☐ Low ☐ Medium ☐ High
	☐ Low ☐ Medium ☐ High
Policies and Procedures	
	☐ Low ☐ Medium ☐ High
	☐ Low ☐ Medium ☐ High
	☐ Low ☐ Medium ☐ High
Security Force	
	☐ Low ☐ Medium ☐ High
	☐ Low ☐ Medium ☐ High
	☐ Low ☐ Medium ☐ High

National Ministries Building Final Security Upgrade Recommendations

1.

2.

3.

4.

Four Main Points of the Operational Resilience Plan Statement

Use this space to write down specific bullet points to summarize the security countermeasure recommendations that you would include in an operational resilience plan statement.

Table 16: Operational Resilience Plan Main Points

PREVENTION

PREPAREDNESS

RESPONSE

RECOVERY

This Page Intentionally Left Blank.