WORKBOOK 16.1: CAPSTONE EXERCISE

Capstone Exercise Overview (30 Minutes)

You will now work in teams to conduct a physical protection system vulnerability analysis for a selected critical infrastructure. Before you begin, here are a few critical pieces of information about how the capstone exercise will be conducted.

This exercise is divided into the following parts:

- **Part 1:** Critical Infrastructure Assessment
- **Part 2:** Critical Infrastructure Assets
- **Part 3:** Threats Estimation
- **Part 4:** Security Inspection and Validation and Site Visit
- **Part 5:** Standoff Distances
- **Part 6:** Security Countermeasure Recommendations and Resilience Plan
- **Part 7:** Team Preparation and Presentations

Capstone Exercise Organizational Matrix

The following information will give you a basic understanding of how each part of the exercise relates to previous course content. Your facilitators will take a few minutes to review the information in the *Capstone Exercise Organizational Matrix Table* before you begin the capstone exercise.

Capstone Exercise Organizational Matrix Table

Part	Reference Module(s)	Time	Refer to:
Part 1	*Module 5: Critical Infrastructure Components*	60 minutes	▪ *Table 1: Vulnerability Analysis Team Assignments* ▪ *Table 2: Assess Critical Infrastructure*
Part 2	*Module 6: Critical Infrastructure Assets*	60 minutes	▪ *Table 3: Critical Assets Identification* ▪ *Table 4: Undesirable Consequences of Critical Asset Loss Analysis* ▪ *Table 5: Threat Spectrum Matrix*

Part	Reference Module(s)	Time	Refer to:
Part 3	*Module 7: Cybersecurity* *Module 10: Analyzing the Threat*	60 minutes	▪ *Table 6: Insider Threat Information Worksheet* ▪ *Table 7: Outsider Threat Information Worksheet* ▪ *Table 8: Estimating Likelihood of Attack Worksheet* ▪ *Threat Analysis Statement*
Part 4	*Module 11: Policies and Procedures* *Module 12: Security Force Operations* *Module 13: Security Technology* *Module 14: Security Inspection and Validation*	60 minutes	▪ *Table 9: Phase 1 — Security Inspection and Validation Planning* ▪ *Table 10: Phase 2 — Security Inspection and Validation Checklist (Policies and Procedures)* ▪ *Table 11: Phase 2 — Security Inspection and Validation Checklist (Security Force)* ▪ *Table 12: Phase 2 — Security Inspection and Validation Checklist (Technology)*
	Transportation to Site	30 minutes	
Site Visit Part 4 (Cont'd.)	*Module 9: Explosives and Critical Infrastructure*	3 hours	▪ *Table 13: Phase 2 — Security Inspection and Validation (Preliminary Recommendations)* ▪ *Table 14: Phase 3 — Security Inspection and Validation Report* ▪ *Table 15: On-Site Measurements*
	Transportation to Classroom	30 minutes	
Part 5	*Module 9: Explosives and Critical Infrastructure*	60 minutes	▪ *Table 16: ATF — Vehicle Bomb Explosion Hazard and Evacuation Distance* ▪ *Table 17: DoD — IED Safe Standoff Distance Sheet*

Part	Reference Module(s)	Time	Refer to:
Part 6	*Module 15: Operational Resilience*	60 minutes	▪ Discussion questions related to recommendations ▪ Operational resilience plan main points: prevention, preparedness, response, and recovery
Part 7	All	2 hours	▪ Discuss final recommendations ▪ Organize all completed tables (*Tables 1–17*) to ensure easy access when called upon by facilitator to share responses ▪ Ensure report is complete and accurately illustrates final recommendations
Team Presentations	All	2 hours	▪ Capstone exercise presentations of results

Timing Icons Used in the Capstone Exercise

To help you and your team complete your work in a timely manner, the following icons will appear in this addendum to indicate approximate times for each part of the exercise:

- 30 minutes 
- 60 minutes 

Capstone Exercise Equipment

At various points in the Capstone Exercise, you will use the following equipment to facilitator information gathering during the exercise and prepare your presentations:

- Laptop
- Capstone exercise presentation template
- USB flash drive
- Clipboards
- Flip-chart easel and paper
- Digital cameras
- Laser range finder

This Page Intentionally Left Blank.

Part 1 of 7: Critical Infrastructure Assessment (1 Hour)

Purpose:	To establish vulnerability analysis team assignments and assess the critical infrastructure
Duration:	60 minutes
Group composition:	Table groups
Equipment:	▪ Laptop ▪ Capstone Exercise Presentation Template ▪ USB Flash Drive ▪ Flip-Chart Easel ▪ Refer to Modules 2 through 15, if needed

Directions:

1. Your facilitator will provide you with a laptop preloaded with a capstone exercise presentation template.
   - You should use this template to complete all parts of this exercise and use this file to project your final presentation.
   - The template includes all of the tables you need to complete your presentation at the end of the exercise.
   - This template is a Microsoft Office PowerPoint file.
   - If you are unfamiliar with how to use Microsoft PowerPoint your facilitator can assist you, or you may choose to follow the format by transferring your tables to flip-chart paper and use the flip chart during your final presentation.
2. Your facilitator will assign you a critical infrastructure for analysis and provide you with information from a site survey report about the selected facility.
3. Write down the name of your critical infrastructure in the space before *Table 1: Vulnerability Analysis Team Assignments* and take notes on the site survey report.
4. Using *Table 1: Vulnerability Analysis Team Assignments*, document your team assignments in the space provided. Ensure that everyone on your team has a role.
   - With the exception of the project manager position, it may be necessary to assign more than one person to a role.
   - You will also need to assign someone familiar with using the laptop computer to maintain documentation of all team responses.
5. Using the Site Survey Report information provided by your facilitator, identify the analysis data provided.
6. Write down your responses in *Table 2: Assess Critical Infrastructure*.
7. It is important to identify any information that is missing or needs additional clarification, just as you would do in a real-world data call review scenario.

8. Write down the missing information or your requests for clarification in the space provided (beneath the section titled **Need for Additional Facility Analysis Information**).
9. Ask your facilitators for guidance, if necessary.

Part 1 Explained

To complete Part 1 of the capstone exercise for a selected critical infrastructure, you will need to receive information from your facilitator about the site, make team member assignments, and begin your analysis of the critical infrastructure.

Site Survey and Intelligence Reports

Your facilitator will provide you with crucial information about the site and threats to the site using the checklist on the following pages.

Determine Vulnerability Analysis Team Assignments

To begin, you will determine vulnerability analysis team assignments. Refer to *Table 1: Vulnerability Analysis Team Assignments*; document your team assignments in the space provided. Ensure that everyone on your team has a role. With the exception of the Project Manager position, it may be necessary to assign more than one person to a role. You will also need to assign someone familiar with using a laptop computer to maintain documentation of all team responses.

Conduct Analysis of Critical Infrastructure

Next, your facilitator will provide you with information from a site survey report that documents initial information about the facility. With your team, discuss and document the types of information you have about the facility and also the information you still need.

You will be able to gather the missing information during your site visit to the facility. Refer to *Table 2: Assess Critical Infrastructure*; ensure you record information related to all six assessment components, as shown in Table 2.

You will have 60 minutes to complete Part 1 of the exercise. Do not share your responses with the class at this time; however, be sure to carefully document your responses, as your group will be asked to present information at the conclusion of the entire capstone exercise.

Site Survey Checklist

✓	Information Needs	Notes
	Facility Title and Local Name	
	Facility Location	
	Facility Description	
	Facility Contacts for Approval of Exercise	
	Facility Tour	
	Facility Layout	
	Facility History	
	Area Crime Types and Levels	
	Facility Construction Type	
	Facility Entrances and Exits	
	Streets that Give Facility Access	
	Types of People that use the Facility	
	Facility General Safety	

✓	Information Needs	Notes
	Facility Fire Safety	
	Money Management on Site	
	Assets on Site	
	Facility External Barriers and Fences	
	Facility Hours of Operation	
	Current Security Force Operations	
	Current Technology Security Measures	
	Current Security Policies and Procedures Used	
	Current Security Force On-Site	
	Previous History with VIPs	
	Other Security Threats in Close Proximity	
	Insider Threat Notes	

Name of Critical Infrastructure: _____

Table 1: Vulnerability Analysis Team Assignments

Name	Role and Area of Expertise
	Project Manager

Name of Critical Infrastructure: _____

Category of Critical Infrastructure: _____

Table 2: Assess Critical Infrastructure

Assess Component	Information Received from Site Survey Report
Physical Conditions	
Facility Operations	
Facility Policies and Procedures	
Regulatory Requirements	
Safety Considerations	
Legal Considerations	

Need for Additional Analysis Information

Whom Should We Talk to at the Facility?

What Pictures Should We Take at the Facility?

This Page Intentionally Left Blank.

Part 2 of 7: Critical Infrastructure Assets (1 Hour)

Purpose:	To identify and prioritize critical assets of a selected critical infrastructure
Duration:	60 minutes
Group composition:	Table groups
Equipment:	▪ Laptop ▪ Capstone Exercise Presentation Template ▪ USB Flash Drive ▪ Flip-Chart Easel ▪ Refer to Modules 2 through 15, if needed

Directions:

1. Using *Table 3: Critical Assets Identification*, identify the critical assets for each category listed (people, information, processes, and equipment).
2. Complete *Table 4: Undesirable Consequences of Critical Asset Loss Analysis* by transferring over the critical assets you identified in Table 3 and record those responses in column 1.
   - To complete columns 2 and 3, assume that all undesirable consequences of critical asset loss are related specifically to any type of terrorist attack.
   - For column 2 (Specify Undesirable Consequences of Critical Asset Loss) and column 3 (Determine Levels of Undesirable Consequences of Critical Asset Loss), apply your team's best collective judgment and knowledge to determine your responses for both of these columns.
   - For column 3, use the values low, medium, or high.
   - Note that you cannot complete column 4 (Probability of Occurrence of Undesirable Events) because information is missing. Discuss the additional information you need to complete column 4 and write it in the space provided after Table 4.
3. Your facilitator will provide you with information from **Intelligence Report 1** about your selected critical infrastructure. Take notes and then discuss the information in the intelligence report**.**
4. Using the additional information from this report, and your team's best collective judgment, go back and complete column 4. Use the values low, medium, or high.
5. Ask your facilitators for guidance, if necessary.
6. Be prepared to share your answers with the class at the conclusion of the capstone exercise.

Part 2 Explained

Using the analysis data you have just identified, continue working with your vulnerability analysis team to complete Part 2 of the capstone exercise. In Part 2, you will identify and prioritize critical assets associated with a selected critical infrastructure facility.

You will have 45 minutes to complete Part 2 of the capstone exercise. Recall that you will not share your responses with the class at this time; however, be sure to carefully document your responses, as your team will be asked to present information from this part of the capstone exercise at the conclusion of the entire exercise.

Name of Critical Infrastructure: _____

Category of Critical Infrastructure: _____

Table 3: Critical Assets Identification

Critical Infrastructure Facility Assets	
People	
Information	
Processes	
Equipment	

Critical Asset Loss Analysis

Name of Critical Infrastructure: _____

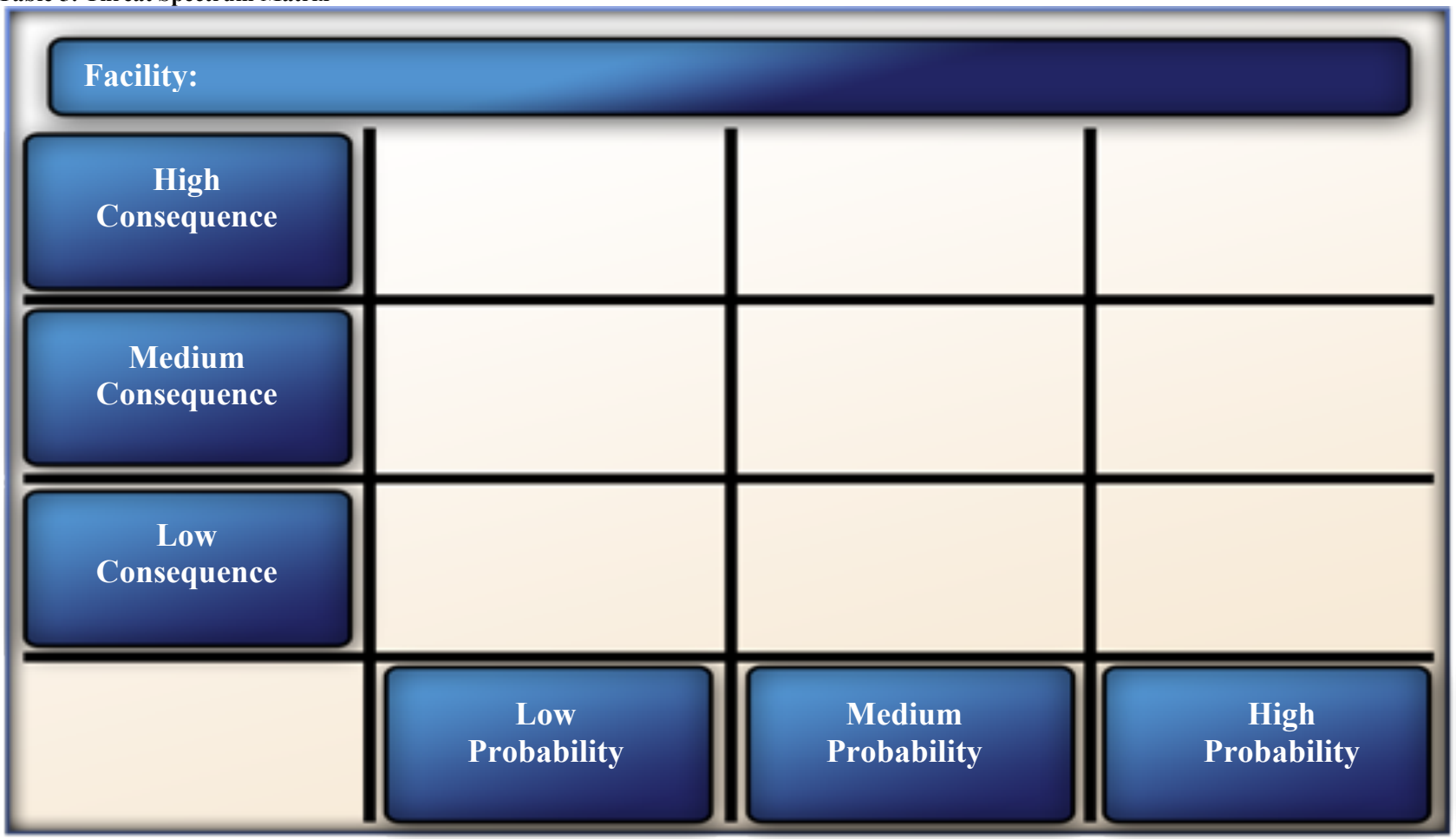
Category of Critical Infrastructure: _____

Table 4: Undesirable Consequences of Critical Asset Loss Analysis

Critical Asset Loss Analysis			
(1) Critical Asset	(2) Undesirable Consequences of Critical Asset Loss	(3) Levels of Undesirable Consequences of Critical Asset Loss	(4) Probability of Occurrence of Undesirable Events
People:			
Information:			
Processes:			
Equipment:			

This Page Intentionally Left Blank.

Table 5: Threat Spectrum Matrix



This Page Intentionally Left Blank.

Part 3 of 7: Threats Estimation (1 Hour)

Purpose:	To examine adversary threats and estimate the likelihood of attack for each threat
Duration:	60 minutes
Group composition:	Table groups
Equipment:	▪ Laptop ▪ Capstone Exercise Presentation Template ▪ USB Flash Drive ▪ Flip-Chart Easel ▪ Refer to Modules 2 through 15, if needed

Directions:

1. Complete *Table 6: Insider Threat Information Worksheet*.
   - Re-examine the information from **Intelligence Report 1** as it relates to Table 6.
   - Discuss information related to insider threats and document your responses in Table 6.
2. Complete *Table 7: Outsider Threat Information Worksheet*.
3. Refer to the information from **Intelligence Report 1** and discuss information related to outsider adversaries and document your responses in Table 7.
4. Complete *Table 8: Estimating Likelihood of Attack Worksheet*.
   - Refer to information from completed Tables 6 and 7.
   - Discuss the estimated likelihood of attack and document your responses in Table 8.
5. Write a threat analysis statement.
   - After you complete the tables listed above, discuss, and prepare your threat analysis statement.
   - Record your threat analysis statement in the space provided at the end of Table 8.
6. Ask your facilitators for guidance, if necessary.

Part 3 Explained

In Part 3 of the capstone 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.

Refer back to the information from **Intelligence Report 1** for the necessary threat information.

You will have 60 minutes to complete Part 3 of the capstone exercise. Recall that you will not share your responses with the class at this time; however, be sure to carefully document your responses, as your team will be asked to present information from this part of the capstone exercise at the conclusion of the entire exercise.

Table 6: 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

This Page Intentionally Left Blank.

Table 7: Outsider Threat Information Worksheet

Threat Type	**Threat 1**
Potential Action (High, Medium, Low)	
Theft	
Sabotage	
Other	
Motivation (High, Medium, Low)	
Political	
Religious	
Social	
Economic	
Personal	
Other	
Tactics	
S=Stealth F=Force D=Deceit	
Capabilities	
Number	
Technical expertise	
Insider assistance	

	Threat 1
Weapons	
Equipment/ Tools	
Transportation	
Other	

Table 8: Estimating Likelihood of Attack Worksheet

Estimating Likelihood of Attack (L_A) Worksheet			
Date:		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.			

Estimating Likelihood of Attack (L_A) Worksheet				
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 =**
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 suggests interest in the facility Score = 2	**Score =**

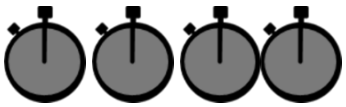
Estimating Likelihood of Attack (L_A) Worksheet				
Category: Current Surveillance	If current intelligence verifies surveillance at the specific site Score = 10	If current intelligence verifies surveillance at other similar facilities in the country or abroad Score = 6	If current intelligence does not involve the specific facility, in the country, or abroad Score = 2	**Score =**
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 =**

Estimating Likelihood of Attack (L_A) Worksheet				
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 =**
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➔				

Threat Analysis Statement

Part 4 of 7: Security Inspection and Validation and Site Visit

Purpose:	To conduct a security inspection and validation for a selected critical infrastructure during a site visit
Duration:	60 minutes and then four hour site visit (including transportation)
Group composition:	Table groups
Equipment:	▪ Laptop ▪ Capstone Exercise Presentation Template ▪ USB Flash Drive ▪ Clipboards ▪ Digital Cameras ▪ Laser Range Finder ▪ Refer to Modules 2 through 15, if needed



Directions:

1. You will begin Part 4 by completing as much information as you can in Tables 9–12 in class.
   - After you complete the tables, your facilitators will explain the procedures for the site visit.
   - You will be provided transportation to the site and allowed three (3) hours on-site to continue your analysis and finalize Tables 9–15.
2. During your site visit, be sure to use your measuring tools to document detailed measurements of the nearest point a vehicle can approach outside of security.
3. Write these measurements in *Table 15: On-Site Measurements*.
   - You will need these measurements to complete Part 5 of the exercise.
   - Locate the nearest point that a vehicle can approach the facility outside of security (public parking or access) and measure the distance between this point and the facility.
4. Refer back to Part 1 of this exercise for the list of photos you want to capture while on-site.
   - Each group will be provided with a digital camera to take photos on-site.
   - Be sure to respect the wishes of the host facility if they ask you not to take pictures in a specific area.
   - With the permission of the on-site representative, use this camera to document the nearest public parking access in relation to the facility, the photos you documented in Part 1 of the exercise, as well as:
   - Entrances and exits
   - Barriers
   - Security measures that appear to be working

- Security measures that need improvement
- Security personnel
- Other critical infrastructure in the immediate area
- Other threat(s) in the immediate area
- Parking area

5. For *Table 9: Phase 1 — Security Inspection and Validation Planning*, discuss what action should be taken prior to conducting the security inspection and validation.
6. Write down these action items in Table 9. For example, prior to conducting the inspection, team members should gather and review pertinent documents describing a selected critical infrastructure facility site (building locations, crucial asset locations, and security force response routes).
7. For *Table 10: Phase 2 — Security Inspection and Validation Checklist (Policies and Procedures)*, refer to *Table 2: Assess Critical Infrastructure* and the *Threat Analysis Statement*, which you completed earlier in this exercise.
   - Consider the identified threat and existing policies and procedures regarding a selected critical infrastructure security.
   - Then, develop questions about policies and procedures that you should ask when the security inspection and validation is conducted during the site visit.
   - During the site visit, be sure to note deficiencies at the end of Table 10.
8. For *Table 11: Phase 2 — Security Inspection and Validation Checklist (Security Force)*, refer to *Table 2: Assess Critical Infrastructure* and the *Threat Analysis Statement*, which you completed earlier in this exercise.
   - Consider the identified threat and existing security countermeasures regarding a selected critical infrastructure security.
   - Then, develop questions about security countermeasures that you should ask when the security inspection and validation inspection is conducted.
   - During the site visit, be sure to note deficiencies at the end of Table 11.
9. For *Table 12: Phase 2 — Security Inspection and Validation Checklist (Technology)*, refer to *Table 2: Assess Critical Infrastructure* and the *Threat Analysis Statement*, which you completed earlier in this exercise.
   - Consider the identified threat and existing technology security countermeasures regarding a selected critical infrastructure security.
   - Then, develop questions about technology security countermeasures that you should ask when conducting the security inspection and validation.
   - During the site visit, be sure to note deficiencies at the end of Table 12.
10. Once on-site, you will complete *Table 13: Phase 2 — Security Inspection and Validation (Preliminary Recommendations)*.
    - You will discuss preliminary security countermeasure recommendations for a selected critical infrastructure facility for all three areas: policies and procedures, security force, and technology.
    - Note that you will also need to list at least three areas where you would recommend limited scope performance testing.
11. Write down your responses at the end of Table 13 in the space provided.

- Recommendations should be directly related to your threat analysis statement and security inspection and validation outcomes.
- Base your recommendations on known information and your team's best collective judgment about feasible and acceptable security countermeasure improvements.

12. For *Table 14: Phase 3 — Security Inspection and Validation Report*, discuss what elements should be included in the security inspection and validation report.
13. Write down your responses in Table 14.
    - For example, after the security inspection and validation has been conducted, the security inspection and validation team is responsible for preparing a report that starts with an executive summary.
    - The first security inspection and validation report element has been entered for you.
14. Ask your facilitators for guidance, if necessary.

Part 4 Explained

For Part 4 of a selected critical infrastructure capstone exercise, continue working with your vulnerability analysis team to prepare to conduct a security inspection and validation of a selected critical infrastructure facility. This will include identifying action items for inspection planning (phase 1), completing the security inspection and validation checklist (phase 2) and identifying elements of the security inspection and validation report (phase 3).

You will have 4 hours total to complete Part 4 of the capstone exercise, including your three hour visit to the selected critical infrastructure. Recall that you will not share your responses with the class at this time; however, be sure to carefully write down your responses, as your team will be asked to present information from this part of the capstone exercise at the conclusion of the entire exercise.

Table 10: Phase 2 — Security Inspection and Validation Checklist (Policies and Procedures)

Questions — Policies and Procedures	Yes ✓	No ✓
1.		
2.		
3.		

Questions — Policies and Procedures	Yes ✓	No ✓
4.		
5.		
6.		
7.		
8.		
9.		
10. Notes (describe deficiencies observed):		

Table 11: Phase 2 — Security Inspection and Validation Checklist (Security Force)

Questions — Security Force	Yes ✓	No ✓
1.		
2.		
3.		
4.		
5.		
6. Notes (describe deficiencies observed):		

Table 12: Phase 2 — Security Inspection and Validation Checklist (Security Technology)

Questions — Security Technology	Yes ✓	No ✓
Closed-Caption Television		
Card Access and Alarm		

Questions — Security Technology	Yes ✓	No ✓
Access Delay		

Questions — Security Technology	Yes ✓	No ✓
Notes (describe deficiencies observed):		

Table 13: Phase 2 — Security Inspection and Validation (Preliminary Recommendations)

Preliminary Security Inspection and Validation Recommendations	
Policies and Procedures	
Security Force	

Preliminary Security Inspection and Validation Recommendations	
Technology and Ability to Delay Access	
Recommendations for Limited Scope Performance Testing (list at least three areas):	

Table 14: Phase 3 — Security Inspection and Validation Report

Security Inspection and Validation Report Elements

Table 15: On-Site Measurements

Distance from the nearest point a vehicle can approach outside of security to the facility:	
Distance from parking area to the building:	
Distance from parking area to the asset(s):	
Distance to other critical infrastructure:	
Distance to other open areas:	
Distance between asset(s):	
Distance to other significant threat(s) (such as hazardous material, train tracks):	

This Page Intentionally Left Blank.

Part 5 of 7: Standoff Distances (1 Hour)

Purpose:	To determine safe standoff distances for a vehicle bomb and suicide bomber attack
Duration:	60 minutes
Group composition:	Table groups
Equipment:	▪ Laptop ▪ Capstone Exercise Presentation Template ▪ USB Flash Drive ▪ Clipboards ▪ Digital Cameras ▪ Laser Range Finder ▪ Refer to Modules 2 through 15, if needed

Directions:

1. Your facilitator will read you **Intelligence Report 2**, which lists specific threat information related to explosives.
2. Take notes and discuss how these threats impact the physical protection system.
3. Refer to *Table 16: ATF — Vehicle Bomb Explosion Hazard and Evacuation Distance* and *Table 17: DoD — IED Safe Standoff Distance Sheet*.
4. Use your measurements taken at the facility and Tables 16–17 to make the following determinations.
   - Is there is sufficient distance to avoid severe damage by a vehicle bomb at the facility? Before making your determination, be sure to consider the facility's current security measures and the largest sized vehicle that can approach the facility given the emplaced security measures.
   - How far inside the critical infrastructure can a suicide bomber approach before a security screen? Is this sufficient distance to avoid severe damage to the critical infrastructure?
5. Write the answers to your determinations in the space provided after Table 17.
6. Ask your facilitators for guidance, if necessary.

Part 5 Explained

Now that you have completed your site visit, you should be able to use the measurements you wrote down in Part 4 and the threat information identified in **Intelligence Report 2** to determine whether there is sufficient distance to avoid severe damage and casualties by a vehicle bomb at the facility and to consider the threat a suicide bomber could cause within the critical infrastructure.

You will have 45 minutes to complete Part 5 of the capstone exercise. Recall that you will not share your responses with the class at this time; however, be sure to carefully document your responses, as your team will be asked to present information from this part of the capstone exercise at the conclusion of the entire exercise.

Table 16: ATF — Vehicle Bomb Explosion Hazard and Evacuation Distance

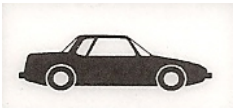
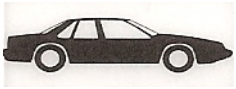
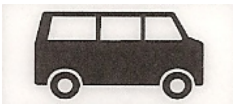
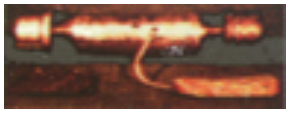
	Vehicle Description	Maximum Explosives Capacity	Lethal Air Blast Range	Minimum Evacuation Distance	Falling Glass Hazard
	Compact Sedan	227 kilograms (In trunk)	30 meters	457 meters	381 meters
	Full Size Sedan	455 kilograms (In trunk)	38 meters	534 meters	534 meters
	Passenger Van or Cargo Van	1,818 kilograms	61 meters	838 meters	838 meters
	Small Box Van (4.3 Meter Box)	4,545 kilograms	91 meters	1,143 meters	1,143 meters
	Box Van or Water/ Fuel Truck	13,636 kilograms	137 meters	1,982 meters	1,982 meters
	Semi-Trailer	27,273 kilograms	183 meters	2,134 meters	2,134 meters

Table 17: DoD — IED Safe Standoff Distance Sheet

	Threat Description	Explosives Mass[1] (TNT equivalent)	Building Evacuation Distance[2]	Outdoor Evacuation Distance[3]
High Explosives (TNT Equivalent)	 Pipe Bomb	2.3 kilograms	21 meters	259 meters
	 Suicide Belt	4.5 kilograms	27 meters	330 meters
	 Suicide Vest	9 kilograms	34 meters	415 meters
	 Briefcase/Suitcase Bomb	23 kilograms	46 meters	564 meters
	 Compact Sedan	227 kilograms	98 meters	457 meters
	 Full Size Sedan	454 kilograms	122 meters	534 meters
	 Passenger or Cargo Van	1,814 kilograms	195 meters	838 meters
	 Small Moving Van or Delivery Truck	4,536 kilograms	263 meters	1,143 meters

	 Semi-trailer	27,216 kilograms	475 meters	2,134 meters
	 Water Truck	13,608 kilograms	375 meters	1,982 meters

	Threat Description	LPG Mass (Volume)[1]	Fireball Diameter[4]	Safe Distance[5]
Liquefied Petroleum Gas (LPG — Butane or Propane)	 Small LPG Tank	9 kg/19 liters	12 meters	48 meters
	 Large LPG Tank	45 kg/95 liters	21 meters	84 meters
	 Commercial or Residential LPG Tank	907 kg/1,893 liters	56 meters	224 meters
	 Small LPG Truck	3,630 kg/7,570 liters	89 meters	356 meters
	 Semi-tanker LPG	18,144 kg/37,850 liters	152 meters	608 meters

(1) Based on the maximum amount of material that could reasonably fit into a container or vehicle. Variations possible.
(2) Governed by the ability of an unreinforced building to withstand severe damage or collapse.
(3) Governed by the greater of fragment throw distance or glass breakage or falling glass hazard distance. These distances can be reduced for personnel wearing ballistic protection. Note that the pipe bomb, suicide belt or vest, and briefcase or suitcase bomb are assumed to have a fragmentation characteristic that requires greater standoff distances than an equal amount of explosives in a vehicle.
(4) Assuming efficient mixing of the flammable gas with ambient air.
(5) Determined by U.S. firefighting practices wherein safe distances are approximately 4 times the flame height. Note that an LPG tank filled with high explosives would require a significantly greater

standoff distance than if it were filled with LPG.

Note: Table 16 and Table 17 provide slightly different calculations, based on rounding up or rounding down of numbers. For example, Table 16 shows that the maximum explosives capacity for a full size sedan is 455 kg; Table 17 shows that the maximum explosives capacity for the same vehicle is 454 kg. This slight difference does not impact accuracy of calculations since they are estimated distances.

Vehicle Bomb Determination

Critical Location:

_____

_____

_____

_____

Vehicle Size and Maximum Explosive Weight: _____

Minimum Safe Distances:

Lethal Air Blast:	
Minimum Evacuation Distance:	
Falling Glass Hazard:	
Building Evacuation Distance:	

Suicide Bomber Determination

How far inside the critical infrastructure can a suicide bomber approach before a security screen? Using Table 17 describe expected explosive weights and evacuation distances. Describe potential casualties.

Minimum Safe Distances:

Minimum Evacuation Distance:	
Building Evacuation Distance:	

Part 6 of 7: Security Countermeasure Recommendation and Operational Resilience Plan (1 Hour)

Purpose:	To determine the main points of an operational resilience plan statement that includes a recommendation based on an immediate request for specific security countermeasure upgrade
Duration:	60 minutes
Group composition:	Table groups
Equipment:	▪ Laptop ▪ Capstone Exercise Presentation Template ▪ USB Flash Drive ▪ Flip-Chart Easel ▪ Digital Cameras ▪ Refer to Modules 2 through 15, if needed

Directions:

1. Based on your findings in Part 5, make recommendations for security upgrades to mitigate the vehicle bomb and suicide bomber threats to the critical infrastructure.
2. Answer the discussion questions that appear in the section titled **Recommendation Discussion Questions**.
3. Write down your answers in the space provided.
4. Determine the main points for your operational resilience plan statement and write them in the space provided.
5. Ask your facilitators for guidance, if necessary.

Part 6 Explained

For Part 6 of the capstone exercise, continue working with your vulnerability analysis team to make recommendations for security countermeasure upgrades to mitigate the vehicle bomb and suicide bomber threats. As you consider your recommendations, discuss how the identified vulnerabilities and recommended security countermeasures will provide the basis for developing an operational resilience plan statement.

You will have 45 minutes to complete Part 6 of the capstone exercise for the selected critical infrastructure. Recall that you will not share your responses with the class at this time; however, be sure to carefully write down your responses, as your team may be asked to present information from this part of the capstone exercise at the conclusion of the entire exercise.

Recommendation Discussion Questions

Question 1: What upgrades do you recommend to mitigate the threat from a large vehicle bomb?

Question 2: What upgrades do you recommend to mitigate the threat from a suicide bomber?

Operational Resilience Plan Main Points

Use this space provided to write down the main points for an operational resilience plan statement that summarizes how your security countermeasure recommendation could enhance operational resilience if an attack like this occurred.

PREVENTION

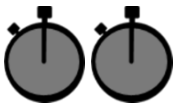
PREPAREDNESS

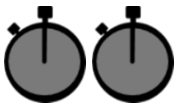
RESPONSE

RECOVERY

Part 7 of 7: Team Preparation (2 Hours) and Presentations (2 Hours)

Purpose:	To make a presentation of your team's complete vulnerability analysis results
Duration:	4 hours (2 hours-preparation; 2 hours-all presentations)
Group composition:	Table groups
Debrief:	Deliver a presentation to your facilitators and fellow participants
Equipment:	▪ Laptop ▪ Capstone Exercise Presentation Template ▪ USB Flash Drive ▪ Flip-Chart Easel ▪ Digital Cameras ▪ Completed Exercise Responses





Directions:

1. Review your final recommendations for your assigned critical infrastructure facility.
   - A good way to do this is to organize all completed tables (Tables 1–17) using the Microsoft Office PowerPoint capstone exercise presentation template loaded on your laptop and check for completeness and legibility.
   - This template is a guide for how to structure your presentation and you may modify it as needed.
   - The facilitators can assist you to project any digital pictures from your laptop during your presentation.
   - You may also use flip-chart paper to draw diagrams to supplement your presentation, as necessary.
2. Use your capstone exercise presentation template as a guide; your report should include the following sections:
   - Authors of the report (your team members) and team assignments
   - Location assessed
   - What critical assets were identified, in what priority
   - Top insider threat
   - Top outsider threat
   - L_A — Likelihood of Attack
   - Threat analysis statement
   - Pictures and overview of security inspection validation
   - Standoff distances
   - Recommendations
   - Operational resilience plan statement

3. Select a spokesperson to present to the class.
   - When directed, your team will be asked to share your report.
   - Make sure the person you select has a clear understanding of your team's collective responses and can provide an accurate description of your work.
4. Following team preparations, each group will have 30 minutes to deliver its presentation and answer questions on their analysis.

Part 7 Explained

For Part 7 of the exercise, continue to work with your vulnerability analysis team to prepare for the exercise presentation. We have provided you with a capstone exercise presentation template on your laptop to use as a guide, but you may use any format you are most comfortable with (such as hand written, or other electronic version such as in Microsoft Word). Your facilitators will help you incorporate your pictures into your presentation.

Each team will have 2 hours to prepare for the presentation portion of the exercise. After all groups have completed their presentations, each group will have 30 minutes to present highlights from their reports. In preparation for the presentation, select one spokesperson from your team to present your findings to the class. All team members should be prepared to answer questions from facilitators and other participants.

Your facilitators will select the order in which the team's present their analysis to the class. After completing the presentation, your facilitators will provide feedback on your analysis.