Unit IV

COURSE TITLE Building Design for Homeland Security **TIME** 105 minutes

UNIT TITLE Vulnerability Assessment

OBJECTIVES

1. Explain what constitutes a vulnerability
2. Identify vulnerabilities using the Building Vulnerability Assessment Checklist
3. Understand that an identified vulnerability may indicate that an asset is vulnerable to more than one threat or hazard and that mitigation measures may reduce vulnerability to one or more threats or hazards
4. Provide a numerical rating for the vulnerability and justify the basis for the rating

SCOPE

The following topics will be covered in this unit:

1. Review types of vulnerabilities, especially single-point vulnerabilities and tactics possible under threats/hazards for which there are no mitigation measures.
2. Various approaches and considerations to determine vulnerabilities – FEMA, Department of Defense, Department of Justice, and Veterans Affairs.
3. A rating scale and how to use it to determine a vulnerability rating. One or more specific examples will be used to focus students on the following activity.
4. Activity: Make an initial identification of vulnerabilities present in the selected Case Study answering the selected Vulnerability Assessment Checklist questions. Then, determine the vulnerability rating for each asset-threat/hazard pair of interest, using the four threats selected for this course (Cyber Attack, Armed Attack, Vehicle Bomb, CBR Attack) as applied against the identified assets. Achieve team concurrence on answers.

REFERENCES

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, pages 1-24 to 1-35 and pages 1-45 to 1-93
2. FEMA 452, *Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings*, pages 3-1 to 3-20
3. Case Study – Appendix A: Suburban, Hazardville Information

Company or Appendix B: Urban, HazardCorp Building as selected
4. Student Manual, Unit IV-A or Unit IV-B as selected (info only – not listed in SM)
5. Unit IV visuals (info only – not listed in SM)

REQUIREMENTS

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings* (one per student)
2. FEMA 452, *Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings* (one per student)
3. Instructor Guide, Unit IV
4. Student Manual (one per student) for selected Case Study
5. Overhead projector or computer display unit
6. Unit IV visuals
7. Risk Matrix poster and box of dry-erase markers (one per team)
8. Chart paper, easel, and markers

UNIT IV OUTLINE

PREPARING TO TEACH THIS UNIT

- **Tailoring Content to the Local Area:** This is a generic instruction unit, but it has great capability for linking to the Local Area. Local Area discussion may be generated as students have specific situations for which they would like to determine vulnerabilities or vulnerability rating prompted by points brought up in the presentation.

The Instructor will discuss generic vulnerabilities found in a building and how tactics possible under threats/hazards can be used against a building. In essence, the students will see the terrorist's thought process for selecting a tactic against a target. Conversely, the students will also be presented vulnerabilities that exist for many tactics. Similar to the ratings presented in Units II and III, various approaches to identify vulnerabilities will be presented.

The students will be introduced to the **Building Vulnerability Assessment Checklist (Table 1-22, pages 1-46 to 1-93, of FEMA 426)** during this unit. Use of the checklist will be reemphasized in Units IX and X covering Chapters 2 and 3 of **FEMA 426**. Note that the vulnerability rating at this point in the assessment process is a rapid screening approach. It provides an initial vulnerability rating based upon mitigation measures already in place against the threat/hazard tactic. It is derived from the interview process with the building management and staff to focus the more in-depth vulnerability assessment using the complete checklist.

- **Optional Activity:** There are no optional activities in this unit, except Student Activity questions that are applicable to the selected Case Study (Suburban or Urban).

- **Activity:** The students will apply the vulnerability identification (or lack of mitigation measures) and vulnerability rating to the Case Study to identify and rate the vulnerabilities found in the Case Study for each asset-threat/hazard pair of interest. The students will quickly review/scan the building data, physical security, building structure, electrical systems, mechanical systems information systems, communications, emergency response, and geographic information system (GIS) portfolio to have a sense of the vulnerabilities at the building being assessed. The **Building Vulnerability Assessment Checklist (Table 1-22, pages 1-46 to 1-93, of FEMA 426)** can be used to capture the sense of potential vulnerabilities and mitigation measures.

- Refer students to their Student Manuals for worksheets and activities.

- Direct students to the appropriate page in the Student Manual.

- Instruct the students to read the activity instructions found in the Student Manual.

- Explain that the vulnerability ratings determined by the team must be transferred to the Risk Matrix poster.

- Tell students how long they have to work on the requirements.

- While students are working, <u>all</u> instructors should closely observe the groups' process and progress. If any groups are struggling, immediately assist them by clarifying the assignment and providing as much help as is necessary for the groups to complete the requirement in the allotted time. Also, monitor each group for full participation of all members. For example,

ask any student who is not fully engaged a question that requires his/her viewpoint to be presented to the group.

- At the end of the working period, reconvene the class.

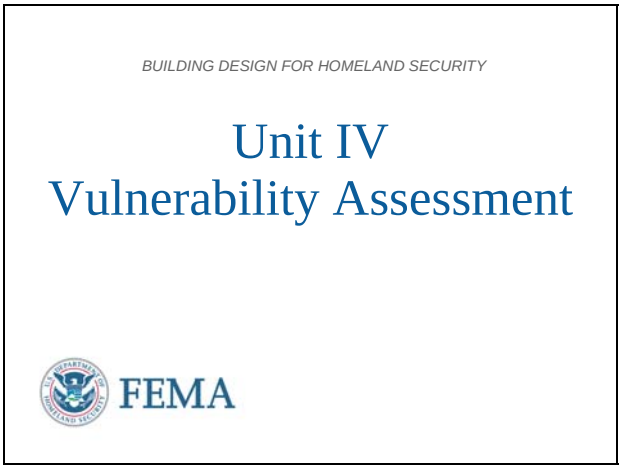
- After the students have completed the assignment, "walk through" the activity with the students during the plenary session. Call on different teams to provide the answer(s) for each question. Then simply ask if anyone disagrees. If the answer is correct and no one disagrees, state that the answer is correct and move on to the next requirement. If there is disagreement, allow some discussion of rationale, provide the "school solution" and move on.

- If time is short, simply provide the "school solution" and ask for questions. Do not end the activity without ensuring that students know if their answers are correct or at least on the right track.

- Ask for and answer questions.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-1

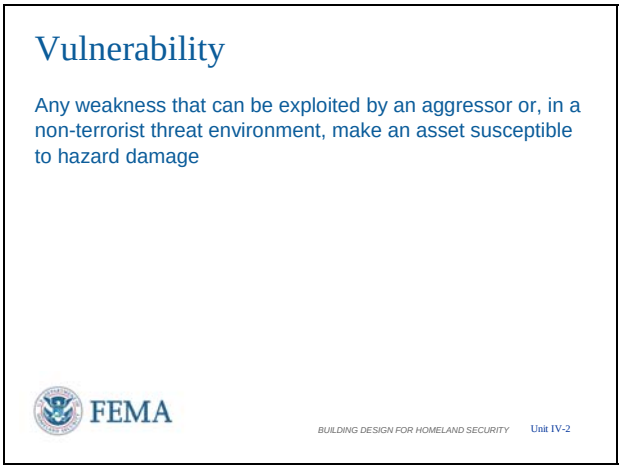


Introduction and Unit Overview

This is Unit IV Vulnerability Assessment. In this unit, we will review types of vulnerabilities, considerations to identifying vulnerabilities, and review a vulnerability rating scale.

This unit also introduces the **FEMA 426 Building Vulnerability Assessment Checklist (Table 1-22, pages 1-46 to 1-93)** to assist in identifying vulnerabilities. This checklist will see extensive use in Units IX, X, and XI (9, 10, and 11).

VISUAL IV-2



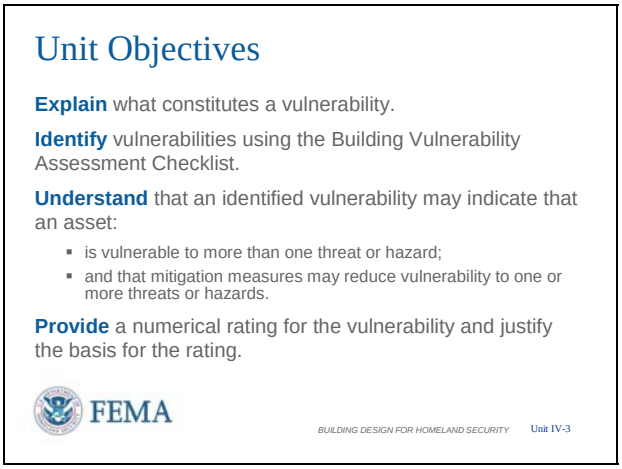
Vulnerability

The definition of vulnerability is any weakness that can be exploited by an aggressor or, in a non-terrorist threat environment, make an asset susceptible to hazard damage.

Essentially it is looking at a tactic against an asset and how successful that tactic can be.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-3



Unit Objectives

At the end of this unit, the students should be able to:

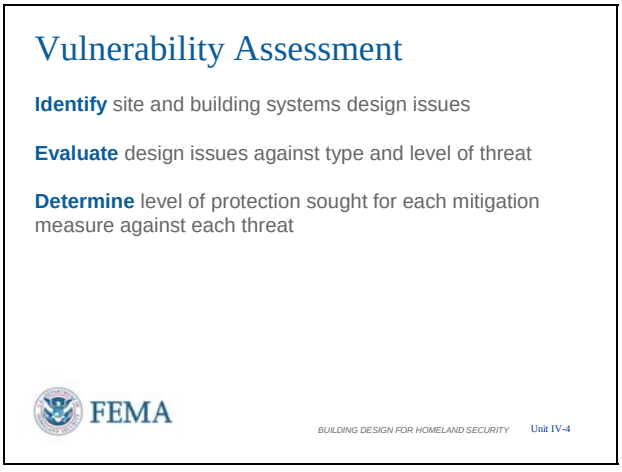
1. Explain what constitutes a vulnerability.

2. Identify vulnerabilities using the **Building Vulnerability Assessment Checklist (Table 1-22, pages 1-46 to 1-93, of FEMA 426)**.

3. Understand that an identified vulnerability may indicate that an asset is vulnerable to more than one threat or hazard, and that mitigation measures may reduce vulnerability to one or more threats or hazards.

4. Provide a numerical rating for the vulnerability and justify the basis for the rating.

VISUAL IV-4



Vulnerability Assessment in this context has three components:

- Identify site and building systems design issues
- Evaluate design issues against type and level of threat
- Determine level of protection sought for each mitigation measure against each threat

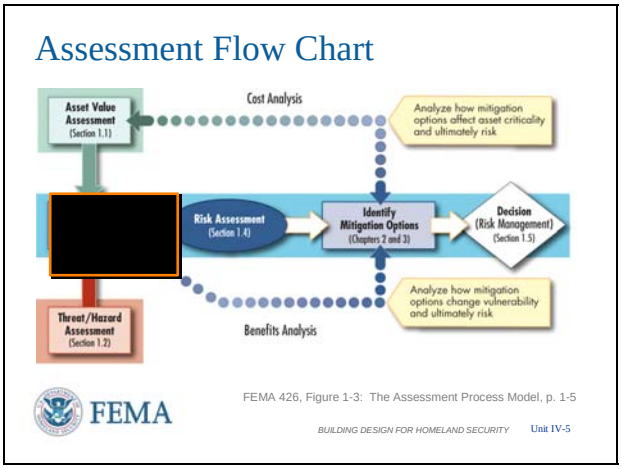
[The goal is to see if existing conditions provide the level of protection desired. Then mitigation measures are sought to achieve the level of protection where it has not been achieved.]

Vulnerability assessments occur at different levels or magnitude of scale, including:

- State / Regional / Business Sector
- Site / Building / Tenant or Occupant

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-5



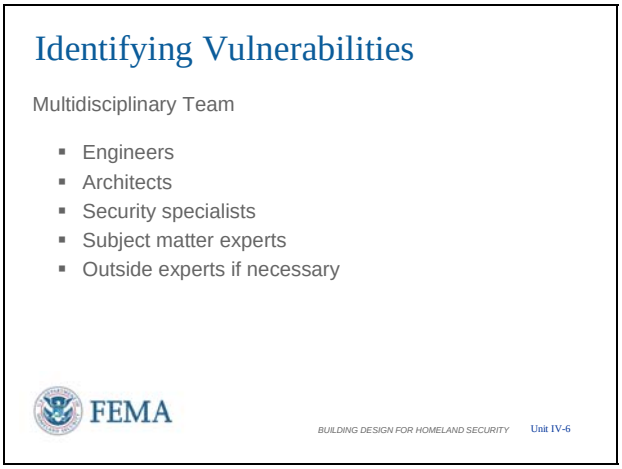
Assessment Flow Chart

Reviewing the Assessment Flow Chart, the vulnerability assessment is the next step in the risk assessment process.

In the prior steps, assets and their respective values were assigned, the threat was analyzed, a Design Basis Threat was established, and a Level of Protection was selected.

The next step is to conduct the vulnerability assessment, which is an in-depth analysis of the building functions, systems, and site characteristics to identify building weaknesses and lack of redundancy, and determine mitigations or corrective actions that can be designed or implemented to reduce the vulnerabilities.

VISUAL IV-6



Identifying Vulnerabilities

Assessing a building's vulnerabilities requires a multidisciplinary team. It should not be conducted solely by an engineer or by a security specialist. Only a balanced team can have an understanding of the identified aggressors or threat/hazards and how they can affect the building's critical functions and infrastructure.

Team members include:

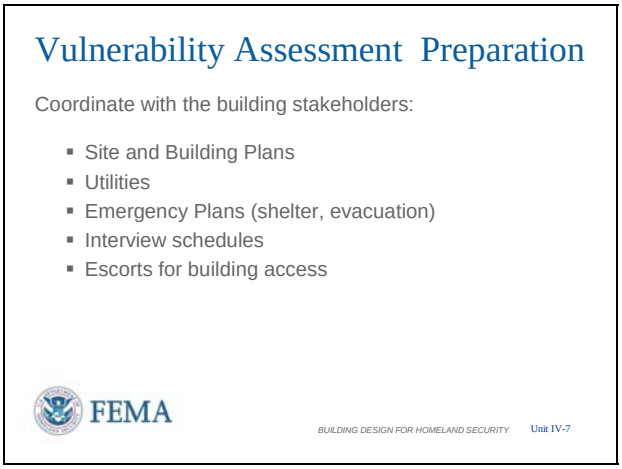
- Engineers
- Architects
- Security specialists
- Subject matter experts
- Outside experts if necessary

Tailor the team to the individual project. A building owner could use his handyman, the local sheriff, his workers, the local volunteer fire department, the service representatives from the local utilities, etc., for an initial

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

assessment. What cannot be answered by this initial team can then be taken to personnel at the next higher level(s) with more expertise and experience in the respective areas.

VISUAL IV-7



Vulnerability Assessment Preparation

After assembling a team, the assessment process starts with a detailed planning and information collection of the site. If possible, the information should be gathered in a GIS format.

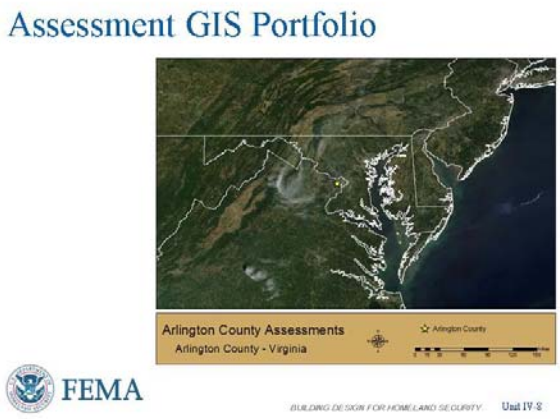
Types of coordination with the building stakeholders include:

- Site and Building Plans
- Utilities
- Emergency Plans (shelter, evacuation)
- Interview schedules [ensure the people who can answer the team assessment questions are available]
- Escorts for building access

Note that no matter how much preparation is done prior to an assessment, the process on site will reveal new information. Conversely, if preparation is not done, much can be missed because the "right" questions may not have been asked on site.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-8



Note: For additional information on HAZUS-MH, refer the student to www.HAZUS.org.

Another important resource is Geospatial One-Stop (www.geo-one-stop.gov), a one-stop source of geospatial information from across the nation. Geospatial information allows decisions to be viewed in a community context (e.g., showing the geographic components of buildings, lifelines, hazards, etc.).

Google Earth is also a powerful tool for the novice to gather like information.

Assessment GIS Portfolio

A technique to organize required information is to develop an Assessment GIS Portfolio. The portfolio is designed to support vulnerability and risk assessments through identification of:

- Critical infrastructure
- Critical nodes within the surrounding area.
- Nearby functions, including emergency response

The data sets are a combination of commercial and government (FEMA – HAZUS-MH, USGS, state, and local data) imagery interpretation, as well as open source transportation, utility, flood plains, and political boundaries.

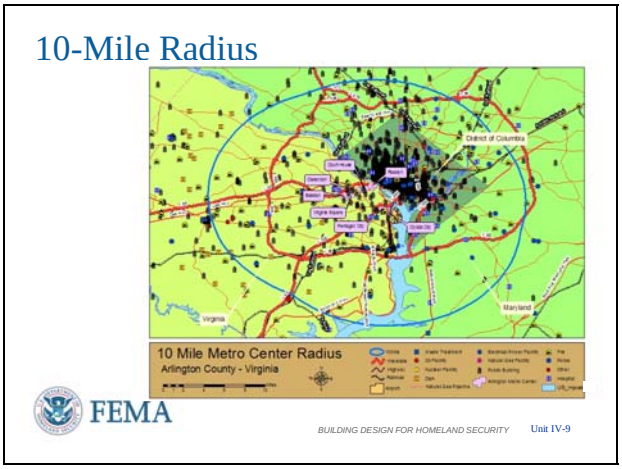
Portfolios are tailored to each individual site.

This slide displays a satellite image of the region with state boundaries delineated. This map provides a general overview for user's initial orientation to a site.

The next series of slides shows how GIS can be used in an outside-to-inside approach to support threat analysis and vulnerability assessments.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

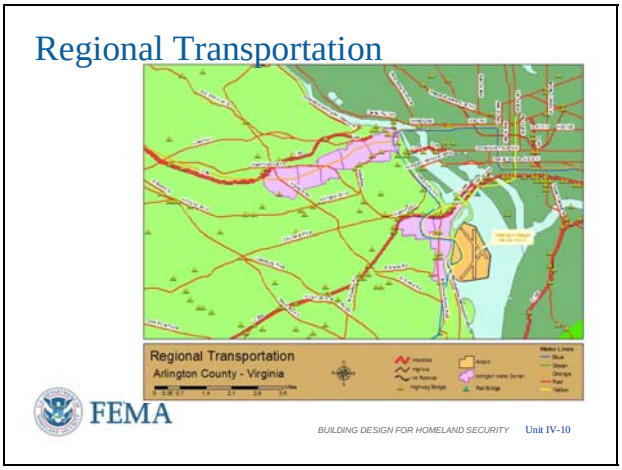
VISUAL IV-9



10-Mile Radius

This map displays infrastructure and features within a 10-mile radius that could have an impact on the site. Features mapped include utilities, major transportation networks, first responders, and government facilities.

VISUAL IV-10

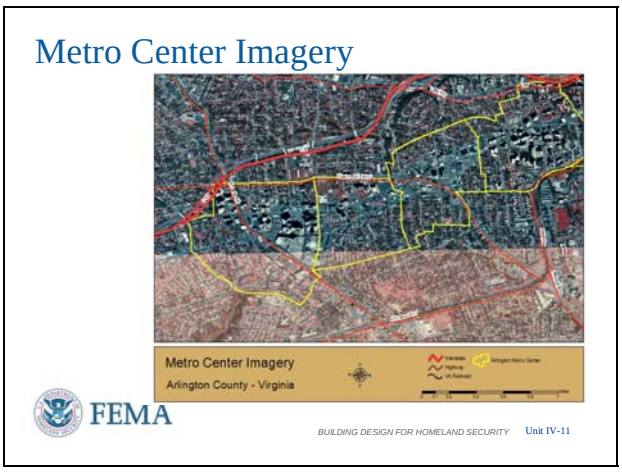


Regional Transportation

The regional transportation map can be used for planning evacuation routes and identifying single-point nodes such as bridges and tunnels.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

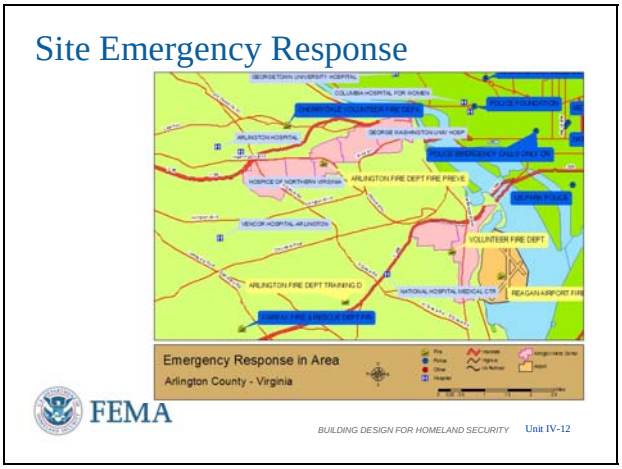
VISUAL IV-11



Metro Center Imagery

Satellite imagery of the region surrounding a site provides users an additional perspective to go with the data sets information. Commercial, industrial, and residential areas can easily be differentiated, as well as rural and urban areas. This map can be used for an overview of the surrounding area and for determining if collateral damage is a significant risk.

VISUAL IV-12

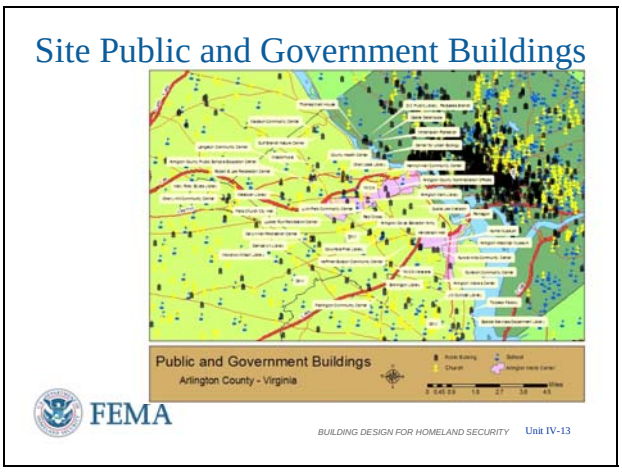


Site Emergency Response

This map displays first responders and hospitals near a site and can be used to estimate response times during an emergency.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

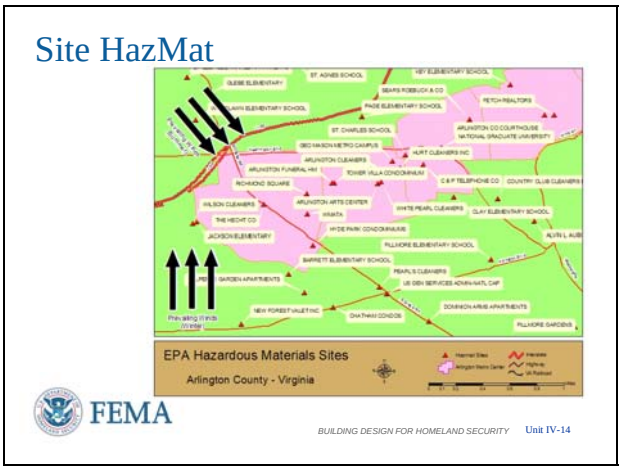
VISUAL IV-13



Site Public/Government Buildings

This map shows the location of government and public buildings in the region, including government facilities, schools, and churches. Government buildings potentially could be the target of terrorist operations. Therefore, the possibility of collateral damage should be considered for sites in close proximity. Additionally, some churches and schools may be designated community shelters and resources during emergencies.

VISUAL IV-14



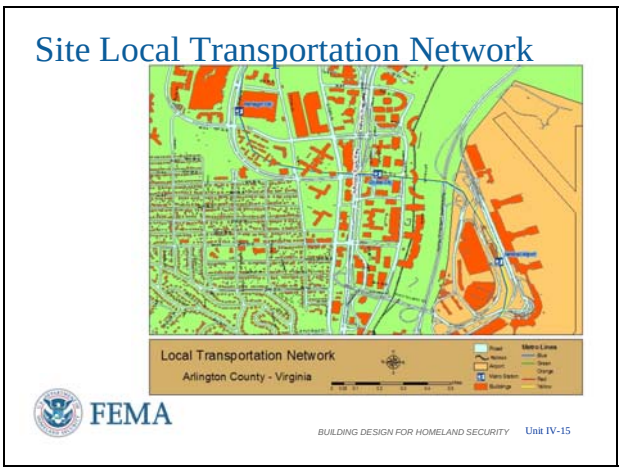
Site HazMat

This map displays hazardous materials (HazMat) sites tracked by various EPA databases. They include large HazMat sites such as refineries and chemical plants, but also include smaller sites with small quantities of chemicals such as schools and dry cleaners. Some sites that contain very small amounts of HazMat are filtered out.

Prevailing wind direction from the National Oceanic and Atmospheric Administration (NOAA) Climatic Data Center is shown to help evaluate the vulnerabilities from surrounding hazards that can be used by a terrorist as a supplemental weapon.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-15



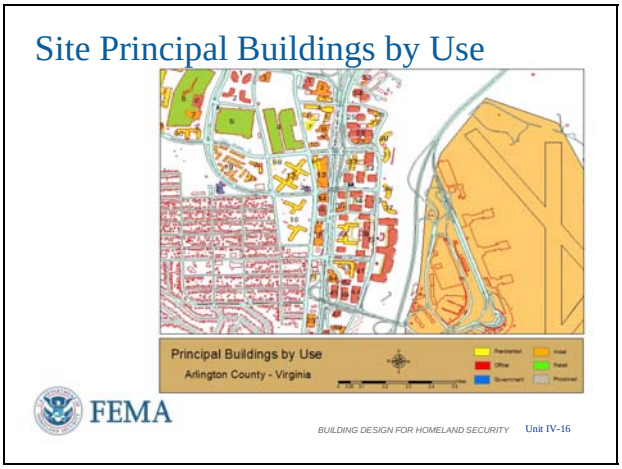
Site Local Transportation Network

The local transportation map provides greater resolution of transportation routes in the local area surrounding a site.

It can be used for planning evacuation routes and alternate routes during for an emergency.

It also shows proximity to routes that do or could carry hazardous materials.

VISUAL IV-16



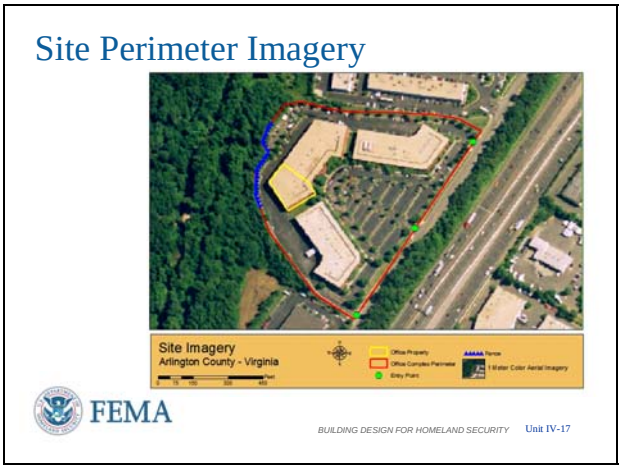
Site Principal Buildings by Use

This map provides a quick overview of the primary use of principal buildings surrounding a site.

It is useful when conducting threat assessments to help identify potential surrounding terrorist targets and the likelihood of collateral damage.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-17

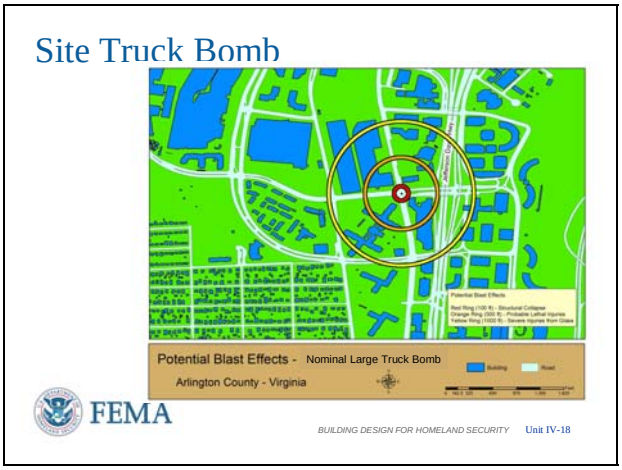


Site Perimeter Imagery

Site imagery gives a view of the site and allows assessors to analyze the layout of the site, including site entry points and building separation.

The imagery can also be integrated with building plans to provide important information for implementing mitigation measures and making other security decisions.

VISUAL IV-18



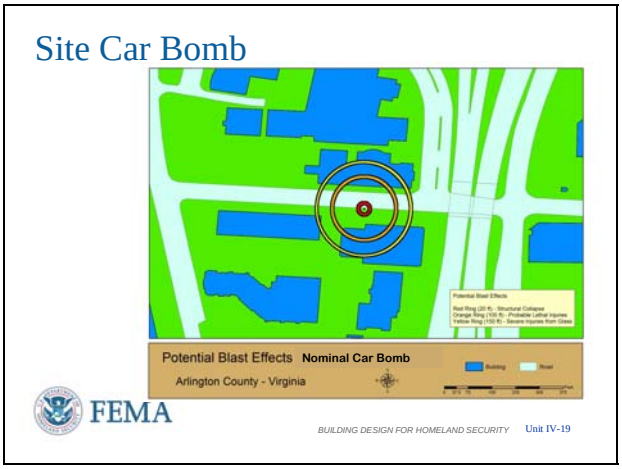
Site Truck Bomb

Displays the potential effects of a nominal truck bomb assuming a nominal building structure.

It is an estimation based on range-to-effects charts and is useful for analyzing vehicular flow and stand-off issues. The results of more accurate site-specific blast analysis can be used to replace the nominal estimations, especially for more accurate cost estimating of mitigation measures.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-19

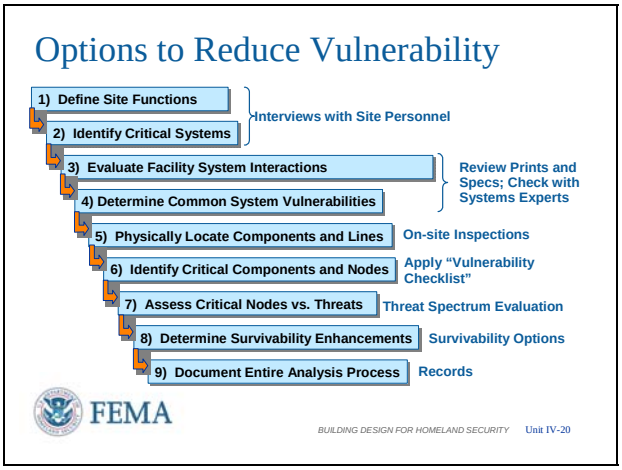


Site Car Bomb

This is an example of the potential blast effects associated with a nominal car bomb against a building with nominal construction.

Obviously, the effects of the car bomb are much less than those from a truck bomb.

VISUAL IV-20



Options to Reduce Vulnerability

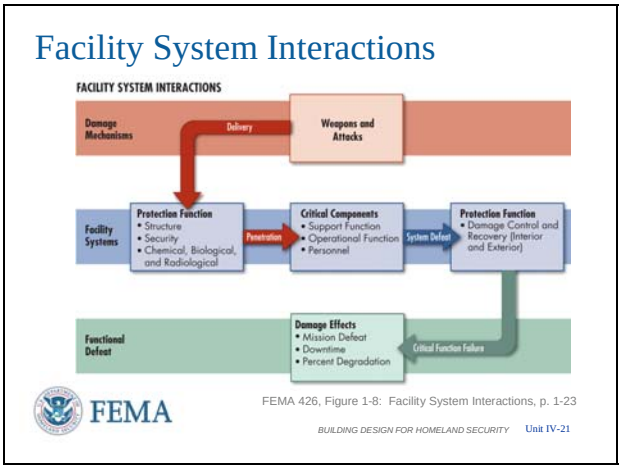
After identifying and collecting information on the site, the multidisciplinary team follows the nine steps listed here:

1. Define Site Functions
2. Identify Critical Systems
3. Evaluate Facility System Interactions
4. Determine Common System Vulnerabilities
5. Physically Locate Components and Lines
6. Identify Critical Components and Nodes
7. Assess Critical Nodes Versus Threats
8. Determine Survivability Enhancements (and Options)
   [Mitigation measures]
9. Document Entire Analysis Process
   [To avoid having to recreate it, but moreso to allow adjustments as threats change and as mitigation measures are implemented so as to track the current state if an attack should occur.]

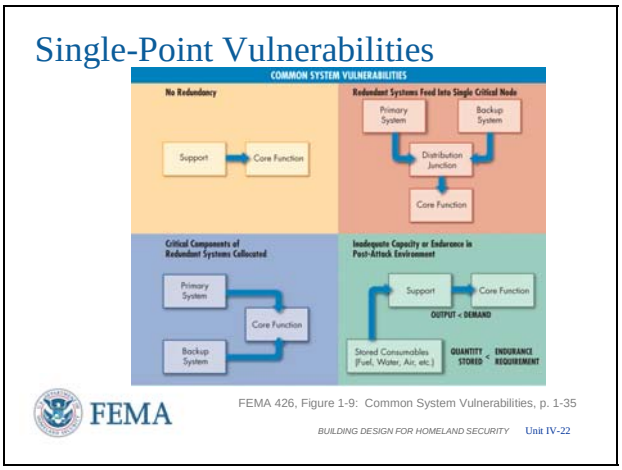
This process is explained in more detail in FEMA 452. For this course, this is an overview of what a more detailed on-site assessment should accomplish.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-21



VISUAL IV-22



Exam Questions #A4 and B3

Single-Point Vulnerabilities are critical functions or systems that lack redundancy and, if damaged by an attack, would result in immediate organization disruption or loss of capability.

Facility System Interactions

Every building or facility can be attacked and damaged or destroyed as illustrated in the flow chart.

A terrorist selects the weapon and tactic that will destroy the building or infrastructure target.

At a site with multiple buildings, **Tables 1-5 through 1-17 in FEMA 426** can be used to rank order these buildings and thus to determine which buildings require more in-depth analysis.

Single-Point Vulnerabilities (SPVs)

The function and infrastructure analysis will identify the geographic distribution within the building and interdependencies between critical assets. Ideally, the functions should have geographic dispersion as well as a recovery site or alternate work location. However, some critical building functions and infrastructure do not have a backup, or will be found collocated. This design creates what is called a Single-Point Vulnerability.

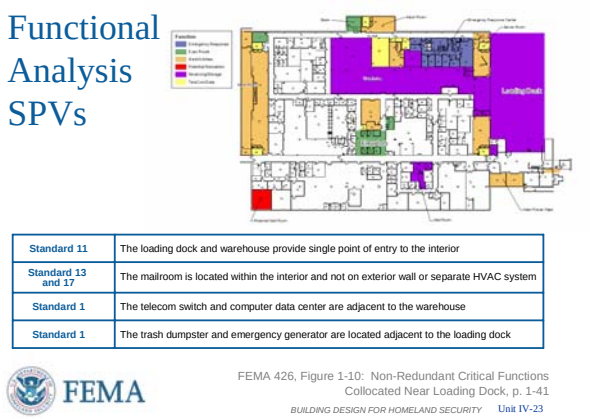
Identification and protection of these Single-Point Vulnerabilities is a key aspect of the assessment process.

This chart provides examples of this concept:

1. No Redundancy
2. Redundant Systems Feed Into Single Critical Node
3. Critical Components of Redundant Systems Collocated
4. Inadequate Capacity or Endurance in Post-Attack Environment

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-23



Functional Analysis SPVs

There are both Functional Analysis SPVs and Infrastructure SPVs.

Functional Analysis SPVs are depicted in this chart. This figure shows an example of a building that has numerous critical functions and infrastructure collocated, which creates a single-point vulnerability.

VISUAL IV-24

Infrastructure Analysis SPVs

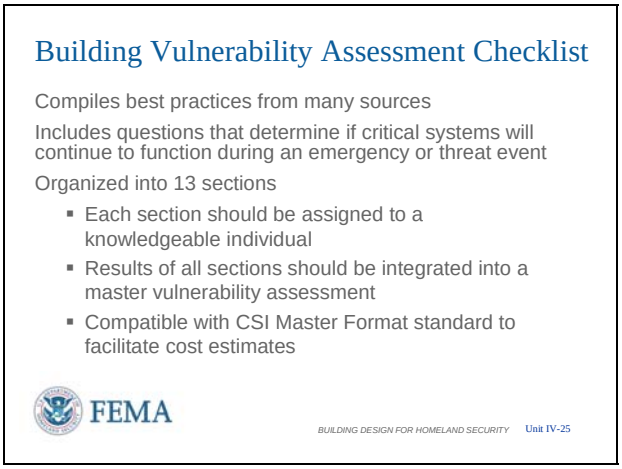
Typical infrastructure SPVs are depicted here:

- Air intakes at ground level
- Ground level drive through drop-off atrium with no anti-vehicle barrier
- Single primary electrical service
- Single telecom switch room in parking garage

Many commercial buildings have collocated electrical, mechanical, and telecom rooms that share a common central distribution core or chase.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-25



The **Building Vulnerability Assessment Checklist** is based on a checklist developed by the Department of Veterans Affairs (VA). The checklist can be used as a screening tool for preliminary design vulnerability assessment. In addition to examining design issues that affect vulnerability, the checklist includes questions that determine if critical systems continue to function in order to enhance deterrence, detection, denial, and damage limitation, and to ensure that emergency systems function during and after a threat or hazard situation.

Building Vulnerability Assessment Checklist

FEMA 426 provides the **Building Vulnerability Assessment Checklist (Table 1-22, pages 1-46 to 1-93)**, which compiles many best practices based on technologies and scientific research to consider during the design of a new building or renovation of an existing building.

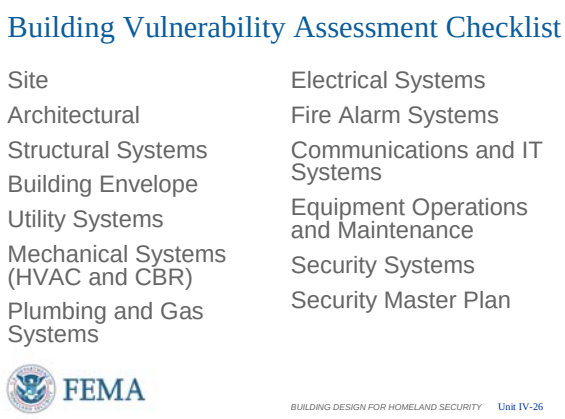
This helps guide the multidisciplinary team through the vulnerability analysis. It allows a consistent security evaluation of designs at various levels, whether accomplished as owner/user or in-depth with technical experts.

The assessment checklist has been used by experienced engineers who were not experienced vulnerability assessors. These engineers commented that although the checklist seemed laborious at first, when they finished assessing multiple sites across the country they felt very confident that they had identified the vulnerabilities and had provided solid recommendations for mitigation measures.

The CSI (Construction Specification Institute) format has other advantages that designers and engineers can develop detailed specifications that communicate requirements to building contractors..

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-26

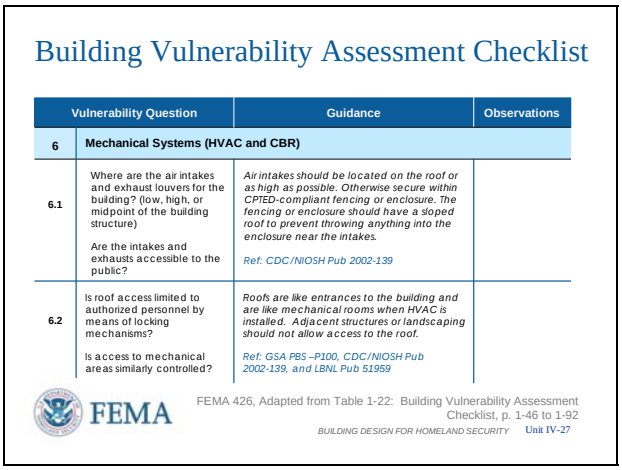


Building Vulnerability Assessment Checklist (Table 1-22, pages 1-46 to 1-93, of FEMA 426)

Each section of the checklist can be assigned to an engineer, architect, or subject matter expert who is knowledgeable and qualified to perform an assessment of the assigned area in order to perform a detailed assessment.

As stated before, an initial assessment can be performed by craftsmen and other knowledgeable people that may provide the decision maker all that is necessary or indicate more expertise is needed in specific areas.

VISUAL IV-27



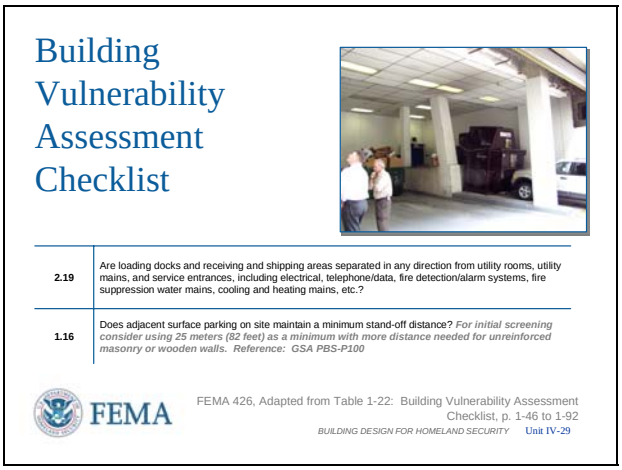
Building Vulnerability Assessment Checklist (Table 1-22, pages 1-46 to 1-93, of FEMA 426)

Each assessor should consider the questions and guidance provided to help identify vulnerabilities and document results in the observations column. Not all possible questions are in the checklist, but it provides a good basis to guide the assessment.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-28

VISUAL IV-29



Building Vulnerability Assessment Checklist (Table 1-22, pages 1-46 to 1-93, of FEMA 426)

Notice that the checklist leads assessment team members to see the same critical functions or infrastructure from different perspectives.

For example, here a parking lot is analyzed by questions from both the site and building envelope sections. (Sections 1 and 4)

This cross analysis is one of the strengths of the methodology.

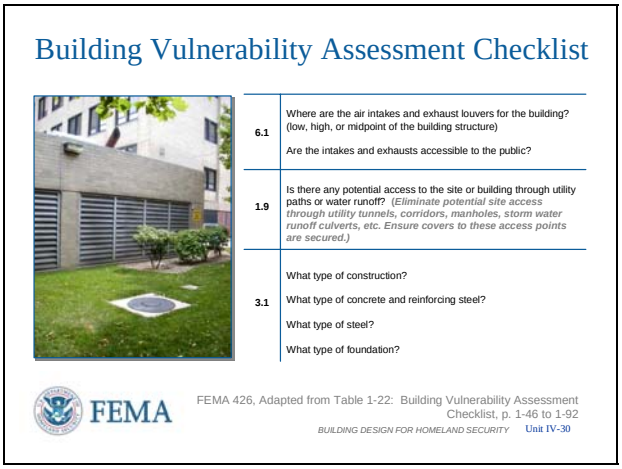
Building Vulnerability Assessment Checklist (Table 1-22, pages 1-46 to 1-93, of FEMA 426)

In this example, the same function, a loading dock, is addressed by different sections (Sections 1 and 2 – Site and Architectural).

The location of the trash dumpster, building overhang, and exposed loading dock columns make this area susceptible to significant blast damage.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-30

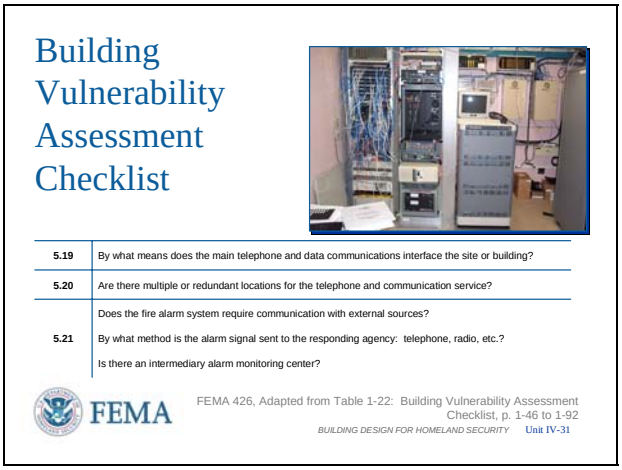


Building Vulnerability Assessment Checklist (Table 1-22, pages 1-46 to 1-93, of FEMA 426)

In this example, the same feature, an air intake, is addressed by questions from three sections:

#1 – Site
#3 – Structural Systems
#6 – Mechanical Systems

VISUAL IV-31



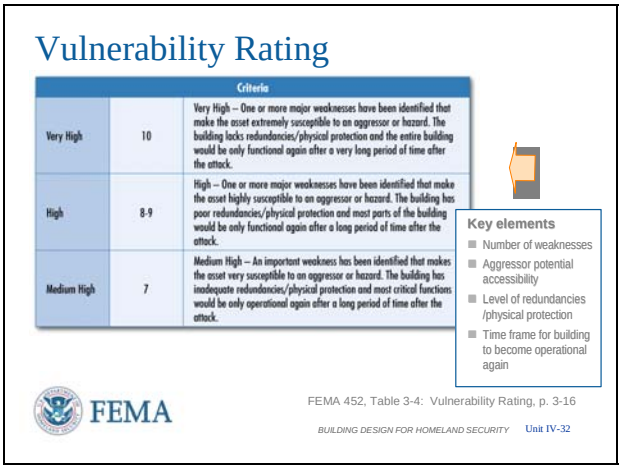
Building Vulnerability Assessment Checklist (Table 1-22, pages 1-46 to 1-93, of FEMA 426)

Section 5 of the **Building Vulnerability Assessment Checklist** addresses Utility Systems.

Utility systems are normally that portion of utilities that is outside the building. However, the demark (demarcation line) can be just inside the building. Up to this point is the responsibility of the utility company. After the demark is part of the building and is handled by other sections in the Building Vulnerability Assessment Checklist.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-32



Vulnerability Rating (1/2)

The results of the 13 assessment sections should be integrated into a master vulnerability assessment in order to provide the basis for determining vulnerability rating numeric values.

In the rating scale of 1 to 10, a rating of 10 means one or more major weaknesses exist to make an asset extremely susceptible to an aggressor's tactics.

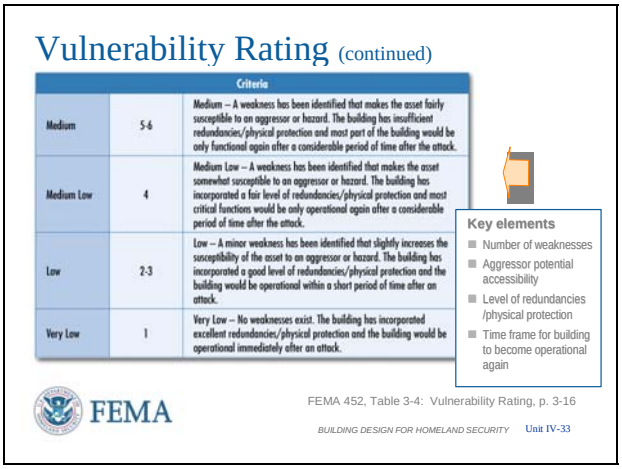
- **Very High** – One or more major weaknesses have been identified that make the asset extremely susceptible to an aggressor or hazard. The building lacks redundancies/physical protection and will not be functional again after an attack.

- **High** – One or more significant weaknesses have been identified that make the asset highly susceptible to an aggressor or hazard. The building has poor redundancies/physical protection and most parts of the building will not be operational until 1 year after an attack.

- **Medium High** – An important weakness has been identified that makes the asset very susceptible to an aggressor or hazard. The building has inadequate redundancies/physical protection and some critical functions will not be operational until 9 months after an attack.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-33



Vulnerability Rating (2/2)

On the other end of the vulnerability rating scale is the rating of 1 which means very low and no weaknesses exist.

- **Medium** – A weakness has been identified that makes the asset fairly susceptible to an aggressor or hazard. The building has insufficient redundancies/physical protection and some critical functions will not be operational until 6 months after an attack.

- **Medium Low** – A weakness has been identified that makes the asset somewhat susceptible to an aggressor or hazard. The building has incorporated a fair level of redundancies/physical protection and the building will be operational 3 months after an attack.

- **Low** – A minor weakness has been identified that slightly increases the susceptibility of the asset to an aggressor or hazard. The building has incorporated good redundancies/physical protection and will be operational a few weeks after an attack.

- **Very Low –** No weaknesses exist. The building has incorporated excellent redundancies/physical protection and will be operational immediately after an attack.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-34

Critical Functions

Function	Cyber attack	Armed attack (single gunman)	Vehicle bomb	CBR attack
Administration				
Asset Value	5	5	5	5
Threat Rating	8	4	3	2
Vulnerability Rating	**7**	**7**	**9**	**9**
Engineering				
Asset Value	8	8	8	8
Threat Rating	8	5	6	2
Vulnerability Rating	**2**	**4**	**8**	**9**

FEMA

FEMA 426, Adaptation of Table 1-20: Site Functional Pre-Assessment Screening Matrix, p. 1-38

BUILDING DESIGN FOR HOMELAND SECURITY Unit IV-34

The Vulnerability Rating is subjective and the assessor has to take into account how well the asset is protected against that threat, if redundancy is in place, and the effect of the tactics and weapons against the asset as it currently exists.

VISUAL IV-35

Critical Infrastructure

Infrastructure	Cyber attack	Armed attack (single gunman)	Vehicle bomb	CBR attack
Site				
Asset Value	4	4	4	4
Threat Rating	4	4	3	2
Vulnerability Rating	**1**	**7**	**9**	**9**
Structural Systems				
Asset Value	8	8	8	8
Threat Rating	3	4	3	2
Vulnerability Rating	**1**	**1**	**8**	**1**

FEMA

FEMA 426, Adaptation of Table 1-21: Site Infrastructure Systems Pre-Assessment Screening Matrix, p. 1-39

BUILDING DESIGN FOR HOMELAND SECURITY Unit IV-35

Critical Functions Matrix

The Vulnerability Rating is entered into the same Critical Functions that we saw in Units II and III.

The Vulnerability Ratings under the Administration Function and under the Engineering Function are highlighted.

Since vulnerability is a measure of the success and effects of employing a threat against asset, the vulnerability varies based upon location, hardening, ability to use the tactic, redundancy, etc.

A medium-high (7) and high (9) Vulnerability Rating was assigned to the Administration Function threat pairs to illustrate an exposed function near exterior walls and entrances.

A range of ratings was assigned for the Engineering Function threat pairs to illustrate a function that is typically in the interior core, but shares common HVAC systems and is likely within a blast damage zone based upon the potential weapon size.

Critical Infrastructure Matrix

The Vulnerability Rating is entered into the same Critical Infrastructure Matrix that we saw in Units II and III.

The Vulnerability Ratings under the Site and Structural Systems are highlighted.

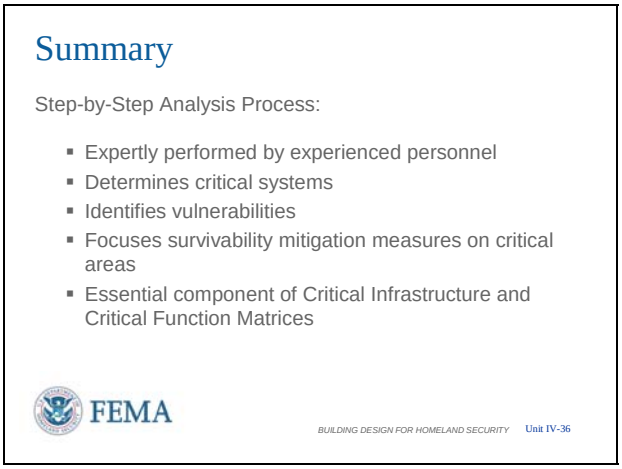
NOTE: It is easier to keep the threat in mind and move between assets to assess vulnerability than it is to keep the asset in mind and move between threats.

Cyber Attack: Rating of 1 for both.

INSTRUCTOR NOTES	CONTENT/ACTIVITY
	• Site: Rating of 1 as no internet connected system in place, like a perimeter access control system, or connection to other accessible media (phone lines). • Structural: Rating of 1 as no electronic systems at all, but could have an active damping system for earthquake or high winds that is accessible over the internet which would give it a rating higher than 1 Armed Attack: • Site: Rating of 7 as it is fairly open but with some obscuration, many manned windows overlooking the parking lots, CCTV coverage, and roving patrols at variable times • Structural: Rating of 1 as this tactic would have no impact upon the structural members Vehicle Bomb • Site: Rating of 9 as a vehicle bomb would cause extensive destruction to site and hinder operations for extended time due to limited access and blowing debris damage to buildings • Structural: Rating of 8 as building is a high-rise and not designed for progressive collapse, but stand-off provides some level of protection. CBR Attack • Site: Rating of 8, because depending upon agent used the access to site could be restricted from hours to years or until decontamination is complete, which would not be a speedy process • Structural: Rating of 1 as agent would not restrict structural system in any fashion in performance of its engineered design

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

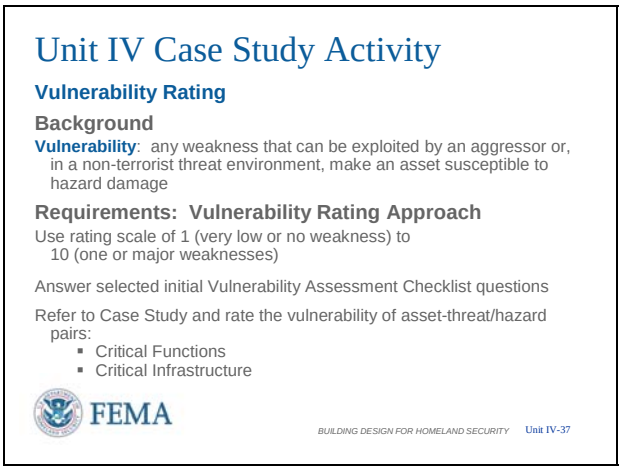
VISUAL IV-36



Summary

- Expertise and experience as required for the level of assessment and the criticality of the building
- Dig deeper in identifying Critical Functions and Critical Infrastructure as the systems interfaces are better understood
- Apply understanding of threats as they interact with assets to identify vulnerabilities and understand benefit of selected mitigation measures
- Apply vulnerability ratings to the Critical Functions and the Critical Infrastructure Matrices based upon how that threat can interact and impact that asset.

VISUAL IV-36



Refer students to the Unit IV Case Study activity in the Student Manual.

At the end of the working session (35 minutes), reconvene the class and facilitate group reporting (plenary group 10 minutes).

Student Activity

Vulnerability is any weakness that can be exploited by an aggressor or, in a non-terrorist threat environment, make an asset susceptible to hazard damage.

Discussion Question

What indicators do you look for to determine if any vulnerability exists in the building design?

Suggested Responses:

- *Critical functions or systems that lack redundancy and if damaged would result in immediate organization disruption or loss of capability ("Single-Point Vulnerability").*
- *Redundant systems feeding into a single critical node.*
- *Critical components of redundant systems collocated.*
- *Inadequate capacity or endurance in post-attack environment.*

INSTRUCTOR NOTES	CONTENT/ACTIVITY
	Activity Requirements: • Working in small groups, answer the worksheet questions from the Building Vulnerability Assessment Checklist and record relevant observations regarding the building and site. • Determine what, if any, vulnerability exists and provide an initial vulnerability rating for all asset-threat / hazard pairs in the Critical Functions and Critical Infrastructure Matrices. • Transfer your team answers to the Risk Matrix poster. Take 35 minutes to complete this part of the activity. **Transition** Unit V will cover Risk Assessment/Risk Management and complete instruction on the risk assessment process. Unit VI will present the FEMA 452 Risk Assessment database as an improvement over the manual process.

UNIT IV-A CASE STUDY ACTIVITY: VULNERABILITY RATING (Suburban Version)

Vulnerability is any weakness that can be exploited by an aggressor or, in a non-terrorist threat environment, make an asset susceptible to hazard damage. Vulnerabilities may include:

- Critical functions or systems that lack redundancy and if damaged would result in immediate organization disruption or loss of capability ("Single-Point Vulnerability")
- Redundant systems feeding into a single critical node
- Critical components of redundant systems collocated
- Inadequate capacity or endurance in post-attack environment

Vulnerability rating requires identifying and rating the vulnerability of each asset-threat/hazard pair of interest. In-depth vulnerability assessment of a building evaluates specific design and architectural features and identifies all vulnerabilities of the building functions and building systems.

Requirements

For an example of how a specific asset is assessed, answer the following questions and record relevant observations on the following table regarding the HIC site and building. Determine what, if any, vulnerability exists:

Section	Vulnerability Question	Guidance	Observations
1.16	Does adjacent surface parking on site maintain a minimum stand-off distance?	The specific stand-off distance needed is based upon the design basis threat bomb size and the building construction. For initial screening, consider using 25 meters (82 feet) as a minimum, with more distance needed for unreinforced masonry or wooden walls. Reference: *GSA PBS-100*	There is no adjacent parking per se, but there is one parking lot or area that any tenant or visitor to the office park can use. Stand-off distance to the front parking lot is less than the 82 feet screening value. Cars or trucks can drive up to the loading dock in the rear.
1.19	Do site landscaping and street furniture provide hiding places?	Minimize concealment opportunities by keeping landscape plantings (hedges, shrubbery, and large plants with heavy ground cover) and street furniture (bus shelters, benches, trash receptacles, mailboxes, newspaper vending machines) away from the building to permit observation of intruders and prevent hiding of packages.	There is no street furniture shown for this building. The landscaping shown is grass and trees are mature/tall enough so that a package cannot be hidden at the base. The hedge along the building drip line may conceal a package, if allowed to get taller or denser. There is no mail or express box and there

		If mail or express boxes are used, the size of the openings should be restricted to prohibit the insertion of packages. Reference: *GSA PBS-100*	is no slot in the glass main entrance door. Due to the size of the building columns, a package could be overlooked.
2.15	Are critical assets (people, activities, building systems and components) located close to any main entrance, vehicle circulation, parking, maintenance area, loading dock, or interior parking? Are the critical building systems and components hardened?	Critical building components include: Emergency generator, including fuel systems, day tank, fire sprinkler, and water supply; Normal fuel storage; Main switchgear; Telephone distribution and main switchgear; Fire pumps; Building control centers; Uninterruptible power supply (UPS) systems controlling critical functions; Main refrigeration and ventilation systems if critical to building operation; Elevator machinery and controls; Shafts for stairs, elevators, and utilities; Critical distribution feeders for emergency power. Evacuation and rescue require emergency systems to remain operational during a disaster and they should be located away from attack locations. Primary and backup systems should be separated to reduce the risk of both being impacted by a single incident if collocated. Utility systems should be located at least 50 feet from loading docks, front entrances, and parking areas. One way to harden critical building systems and components is to enclose them within hardened walls, floors, and ceilings. Do not place them near high-risk areas where they can receive collateral damage. Reference: *GSA PBS-100*	This building is not large enough to maintain separation distances. Attack from the front of the building could primarily impact office space. Attack from the rear would affect critical utilities and, through the loading dock area, the heart of the company – the computer center. No critical components are hardened as seen by the natural gas and electric service to the building. The UPS, mechanical and electrical room, and the diesel generator could be affected by a single bomb less than 50 feet from all these areas or taken out by a single wayward truck.
2.16	Are high value or critical assets located as far into the interior of the	Critical assets, such as people and activities, are more vulnerable to hazards when on an exterior building wall or	People are located along the exterior wall at the front of the building. The secure space has the best interior space location

	building as possible and separated from the public areas of the building?	adjacent to uncontrolled public areas inside the building. Reference: *GSA PBS-100*	– not on an exterior wall, as does the conference room. The office space acts as the buffer between the critical functions in the back and the public area of the building at the main entrance.
4.2	Is there less than 40 percent fenestration openings per structural bay? Is the window system design on the exterior façade balanced to mitigate the hazardous effects of flying glazing following an explosive event? (glazing, frames, anchorage to supporting walls, etc.)	The performance of the glass will similarly depend on the materials. Glazing may be single pane or double pane, monolithic or laminated, annealed, heat strengthened, or fully tempered. The percent fenestration is a balance between protection level, cost, the architectural look of the building within its surroundings, and building codes. One goal is to keep fenestration to below 40 percent of the building envelope vertical surface area, but the process must balance differing requirements. A blast engineer may prefer no windows; an architect may favor window curtain walls; building codes require so much fenestration per square footage of floor area; fire codes require a prescribed window opening area if the window is a designated escape route; and the building owner has cost concerns. Ideally, an owner would want 100 percent of the glazed area to provide the design protection level against the postulated explosive threat (design basis threat – weapon size at the expected stand-off distance). However, economics and geometry may allow 80 percent to 90 percent due to the statistical differences in the manufacturing process for glass or the angle of incidence of the blast wave upon upper story windows (4th floor and higher). Reference: *GSA PBS-100*	Windows are only used in the office space area of the building. Although dimensions are not given, it looks like the glass is at least 75 percent of the wall area between building structural columns. The window system is a standard commercial installation and thus, the glass, framing, and anchorage are expected to be insufficient for the design basis threat at the available stand-off. One benefit is that there are windows only on two sides of the building.

HIC Critical Functions Vulnerability Rating

Requirements

Refer to the HIC Case Study and rate the vulnerability of the following asset-threat/hazard pairs of interest.

Function	Cyber Attack	Armed Attack	Vehicle Bomb	CBR Attack
1. Administration	4	8	8	6
2. Engineering/IT Technicians	4	6	8	6
3. Loading Dock/ Warehouse	2	8	8	6
4. Data Center	3	4	8	6
5. Communications	3	4	8	6
6. Security	4	8	8	6
7. Housekeeping	2	2	8	6

HIC Critical Infrastructure Vulnerability Rating

Requirements

Refer to the HIC Case Study and rate the vulnerability of the following asset-threat/hazard pairs of interest.

Infrastructure	Cyber Attack	Armed Attack	Vehicle Bomb	CBR Attack
1. Site	1	8	8	6
2. Architectural	1	8	8	1
3. Structural Systems	1	8	8	1
4. Envelope Systems	1	8	8	1
5. Utility Systems	5	7	6	1

6. Mechanical Systems	5	7	8	7
7. Plumbing and Gas Systems	1	3	8	1
8. Electrical Systems	5	7	8	5
9. Fire Alarm Systems	2	3	8	3
10. IT/Communications Systems	7	4	8	6

UNIT IV-B CASE STUDY ACTIVITY: VULNERABILITY RATING (Urban Version)

Vulnerability is any weakness that can be exploited by an aggressor or, in a non-terrorist threat environment, make an asset susceptible to hazard damage. Vulnerabilities may include:

- Critical functions or systems that lack redundancy and if damaged would result in immediate organization disruption or loss of capability ("Single-Point Vulnerability")
- Redundant systems feeding into a single critical node
- Critical components of redundant systems collocated
- Inadequate capacity or endurance in post-attack environment

Vulnerability rating requires identifying and rating the vulnerability of each asset-threat/hazard pair of interest. An in-depth vulnerability assessment of a building evaluates specific design and architectural features and identifies all vulnerabilities of the building functions and infrastructure systems.

Requirements

1. Answer the following Building Vulnerability Checklist Questions and record relevant observations in the table regarding the HZC site and building information from the Appendix B Case Study. Determine if the observation indicates that any vulnerabilities exist:

2. Complete the tables for HZC Critical Functions Vulnerability Rating and HZC Critical Infrastructure Vulnerability Rating by filling in the initial vulnerability rating for the asset-threat/hazard pairs.

3. Transfer the vulnerability ratings to the Risk Matrix poster after reaching team consensus on the team answer.

Section	Vulnerability Question	Guidance	Observations
1.16	Does adjacent surface parking on site maintain a minimum stand-off distance?	The specific stand-off distance needed is based upon the design basis threat bomb size and the building construction. For initial screening, consider using 25 meters (82 feet) as a minimum, with more distance needed for unreinforced masonry or wooden walls. Reference: *GSA PBS-100*	On the east side of the plaza is a drop off zone where no parking is allowed and building stand-off is 80 feet. On the north and west sides of the building for the whole building block, parking is restricted to government vehicles only with designated parking spaces. Double parking next to the government vehicles provides 15 feet of stand-off on the north side and 10 feet of stand-off on the west. Commercial

			parking is allowed on the south side in support of the Loading Dock and stand-off is 10 feet.
1.19	Do site landscaping and street furniture provide hiding places?	Minimize concealment opportunities by keeping landscape plantings (hedges, shrubbery, and large plants with heavy ground cover) and street furniture (bus shelters, benches, trash receptacles, mailboxes, newspaper vending machines) away from the building to permit observation of intruders and prevent hiding of packages. If mail or express boxes are used, the size of the openings should be restricted to prohibit the insertion of packages. Reference: *GSA PBS-100*	There is no site landscaping or street furniture shown for this building, although the plaza on the east side would be suitable for planters and benches to establish and maintain stand-off.
2.15	Are critical assets (people, activities, building systems and components) located close to any main entrance, vehicle circulation, parking, maintenance area, loading dock, or interior parking? Are the critical building systems and components hardened?	Critical building components include: Emergency generator, including fuel systems, day tank, fire sprinkler, and water supply; Normal fuel storage; Main switchgear; Telephone distribution and main switchgear; Fire pumps; Building control centers; Uninterruptible power supply (UPS) systems controlling critical functions; Main refrigeration and ventilation systems if critical to building operation; Elevator machinery and controls; Shafts for stairs, elevators, and utilities; Critical distribution feeders for emergency power. Evacuation and rescue require emergency systems to remain operational during a disaster and they should be located away from attack locations. Primary and backup systems should be separated to reduce the risk of both being impacted by a single incident if collocated. Utility systems should be located at least 50 feet from loading docks, front entrances, and parking areas.	The building administration and electrical utilities are located on the first floor near the street and the entrance to underground parking. Utilities enter the site underground and transit the underground parking levels before reaching the vertical risers and proceeding to the mechanical floors, which start on the 4th floor. This provides much protection for utilities and backup generators by keeping them well above street level. There is one fuel tank underneath the loading dock. The building core places most critical assets toward the interior of the building with the exception of that above, with elevators and stairs having slightly less than 50 foot separation distance from the loading dock. No critical building systems or components are specifically hardened.

		One way to harden critical building systems and components is to enclose them within hardened walls, floors, and ceilings. Do not place them near high-risk areas where they can receive collateral damage. Reference: *GSA PBS-100*	
2.16	Are high value or critical assets located as far into the interior of the building as possible and separated from the public areas of the building?	Critical assets, such as people and activities, are more vulnerable to hazards when on an exterior building wall or adjacent to uncontrolled public areas inside the building. Reference: *GSA PBS-100*	Tenants occupy floors six and higher which removes them from the primary uncontrolled public areas on the first through third floors. However, many tenants require uncontrolled public access to transact business. Except for building administration and electrical utilities, no critical assets are near an outside wall on the first three floors. However, the underground parking is open to the public and all utilities transit the underground parking levels.
4.2	Are there less than 40 percent fenestration openings per structural bay? Is the window system design on the exterior façade balanced to mitigate the hazardous effects of flying glazing following an explosive event? (glazing, frames, anchorage to supporting walls, etc.)	The performance of the glass will similarly depend on the materials. Glazing may be single pane or double pane, monolithic or laminated, annealed, heat strengthened, or fully tempered. The percent fenestration is a balance between protection level, cost, the architectural look of the building within its surroundings, and building codes. One goal is to keep fenestration to below 40 percent of the building envelope vertical surface area, but the process must balance differing requirements. A blast engineer may prefer no windows; an architect may favor window curtain walls; building codes require so much fenestration per square footage of floor area; fire codes require a prescribed window opening area if the window is a designated escape	The building uses window curtain walls for its exterior envelope which places the fenestration (windows) at close to 100 percent. Some of the windows are spandrel elements (not used for vision, but cover structural members or mechanical floors where vision is not desired). The glass has varying thickness and strength with safety levels provided at street level to avoid injury to pedestrian traffic and strength increasing with elevation due to wind loading requirements.

		route; and the building owner has cost concerns. Ideally, an owner would want 100 percent of the glazed area to provide the design protection level against the postulated explosive threat (design basis threat – weapon size at the expected stand-off distance). However, economics and geometry may allow 80 percent to 90 percent due to the statistical differences in the manufacturing process for glass or the angle of incidence of the blast wave upon upper story windows (4th floor and higher). Reference: *GSA PBS-100*	

HZC Critical Functions Vulnerability Rating

Requirements

Refer to the Appendix B Case Study and rate the vulnerability of the following asset-threat/hazard pairs of interest. Transfer vulnerability ratings to the Threat Matrix and achieve team consensus on the answers.

Function	Cyber Attack	Armed Attack	Vehicle Bomb	CBR Attack
1. Administration	5	6	10	6
2. Engineering / IT Technicians	3	3	9	5
3. Loading Dock / Warehouse	2	6	10	7
4. Data Center	7	3	10	5
5. Communications	7	3	10	5
6. Security	7	7	10	7
7. Housekeeping	1	2	8	5

Cyber Attack is based upon the level of interaction the function has with the internet. Thus, the Loading Dock and Housekeeping have very little, whereas the Data Center, Communications, and Security are all co-located and have various internet connections. Engineering/IT Technicians is more the building operations and maintenance personnel whose systems are normally stand-alone or that allow access from home through passwords and firewalls to monitor and adjust parameters of concern.

Armed Attack is based upon target value, location, and accessibility. Thus, Administration and Loading Dock are relatively high, along with Security which is readily identified. Engineering is normally throughout the building in a random manner and behind locked doors on mechanical floors. Communications and Data Center are behind another layer of protection within the Administration area on the first floor, thus, are less vulnerable than Administration as a whole. Building Management offices are also located in the public access area of the third floor, which increases their vulnerability.

Vehicle Bomb demonstrates the indiscriminate nature of this tactic which has a global effect on the building. Engineering and housekeeping are less vulnerable as they are further from the vehicle bomb, either by location or time of day (housekeeping normally would do their work

before or after business hours on the first three floors for example, as well as in offices on upper floors).

CBR Attack is also a global effect upon the building, with variation based upon location within the building, time of day, and layers of protection available for an external release.

HZC Critical Infrastructure Vulnerability Rating

Requirements

Refer to the Appendix B Case Study and rate the vulnerability of the following asset-threat/hazard pairs of interest. Transfer vulnerability ratings to the Threat Matrix and achieve team consensus on the answers.

Infrastructure	Cyber Attack	Armed Attack	Vehicle Bomb	CBR Attack
1. Site	2	5	9	7
2. Architectural	1	5	10	5
3. Structural Systems	1	1	10	1
4. Envelope Systems	1	6	10	1
5. Utility Systems	5	1	8	1
6. Mechanical Systems	4	2	7	7
7. Plumbing and Gas Systems	4	1	7	3
8. Electrical Systems	4	3	9	3
9. Fire Alarm Systems	4	1	7	2
10. IT / Communications Systems	9	2	10	3

Cyber Attack is based upon connectivity to the internet. The Site has some access control and security systems that increase its vulnerability. Architectural, Structural Systems, and Envelope Systems have no internet connectivity. Utility Systems coming to the site are controlled by their respective companies and have more points of attack than the HZC building. Internal building

utility systems have various levels of computer controls and access to internet. Finally, IT/Communications Systems have the greatest connectivity, and, thus, the greatest vulnerability.

Armed Attack follows the same logic as critical functions, except that damage to the infrastructure by an armed attack has a greater consideration. Accessibility to the Site as a whole, layout of functions with public access under Architectural, and the fragility of the Envelope Systems to a projectile all receive higher vulnerability ratings. Utility Systems and building systems that are well hidden are given the lowest rating, but Electrical Systems, Mechanical Systems, and IT/Communications Systems which are readily identifiable have slightly higher ratings with respectively greater damage caused by a single projectile.

Vehicle Bomb exhibits its global effects nature with proximity to bomb raising the vulnerability rating. The IT/Communications and Electrical Utilities on the first floor increase their vulnerability. Site to Envelope Systems consider that same proximity to an explosion just outside the exterior wall of the building. The remaining systems also receive high ratings due to the size of the design basis threat, the lack of hardening, and the public access to the underground parking.

CBR Attack is also global, but takes into account the effect of the CBR agents on the equipment, its operation, and the accessibility of operations and maintenance personnel to ensure system operations. Thus, the Site for general accessibility, Architectural due to the layout of functions and accessibility and Mechanical Systems get higher ratings. Structural Systems, Envelope Systems, and Utility Systems get the lowest rating as there will be no effect and access for operations is negligible. The remaining assets receive slightly higher ratings as these may require access to ensure operation shortly after the CBR attack.

This page intentionally left blank