

Unit IV (C)

COURSE TITLE	Building Design for Homeland Security for Continuity of Operations (COOP) Train-the-Trainer	TIME 105 minutes
---------------------	---	-------------------------

UNIT TITLE	Vulnerability Assessment
-------------------	--------------------------

OBJECTIVES	<ol style="list-style-type: none">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	<p>The following topics will be covered in this unit:</p> <ol style="list-style-type: none">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 (primarily), with inputs from Departments of Defense, Justice, and Veterans Affairs.3. A rating scale and how to use it to determine a vulnerability rating.4. Activity: Determine the vulnerability rating, with rationale, 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	<ol style="list-style-type: none">1. FEMA 426, <i>Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings</i>, pages 1-24 to 1-35 and pages 1-45 to 1-932. FEMA 452, <i>Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings</i>, pages 3-1 to 3-203. Case Study – Appendix C: COOP, Cooperville Information / Business Center4. Student Manual, Unit IV (C) (info only – not listed in SM)5. Unit IV (C) visuals (info only – not listed in SM)
-------------------	--

REQUIREMENTS	<ol style="list-style-type: none"> 1. FEMA 426, <i>Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings</i> (one per student) 2. FEMA 452, <i>Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings</i> (one per student) 3. Instructor Guide, Unit IV (C) 4. Student Manual, COOP Case Study (C) (one per student) 5. Overhead projector or computer display unit 6. Unit IV (C) visuals 7. Risk Matrix poster and box of dry-erase markers (one per team) 8. Chart paper, easel, and markers (one per team)
---------------------	---

UNIT IV (C) OUTLINE	<u>Time</u>	<u>Page</u>
IV. Vulnerability Assessment	105 minutes	IG IV-C-1
1. Introduction and Unit Overview	5 minutes	IG IV-C-5
2. Identification of Vulnerabilities	30 minutes	IG IV-C-7
3. Rating of Vulnerabilities	10 minutes	IG IV-C-22
4. Summary, Vulnerability Rating Considerations, Student Activity, and Transition	5 minutes	IG IV-C-26
5. Activity: Vulnerability Rating (Version (C) COOP) [30 minutes for students, 15 minutes for review]	45 minutes	IG IV-C-29

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.
- **Optional Activity:** There are no optional activities in this unit.
- **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 (Unit #) 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, all 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.

Editor Note: Two methods have been used in Instructor Guides to ensure the slide designation and slide thumbnail in the left column aligns with the Content/Activity in the right column.

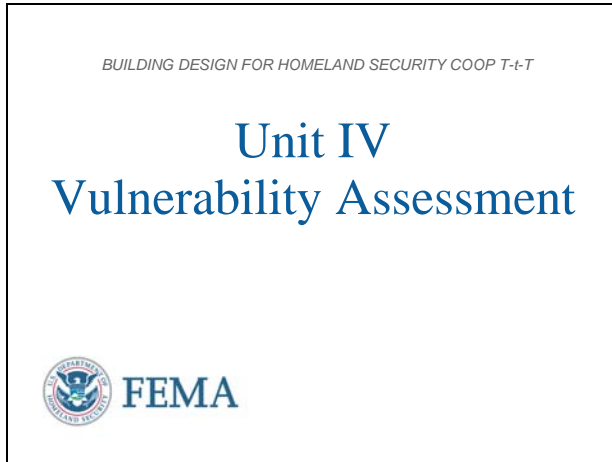
- (1) Highlight row by placing cursor in left column until arrow shifts to right, Tab <Insert>, <Break>, <select Page Break>, <OK>
- (2) Highlight row as in (1), right click on highlighted row for menu, <Table Properties>, Tab <Row>, remove check in box <Allow row to break across pages>
- (3) Alternate for (2), highlight row, click on <Table> at top of screen, <Table Properties> and continue like (2)

This page intentionally left blank

INSTRUCTOR NOTES

CONTENT/ACTIVITY

VISUAL IV-C-1

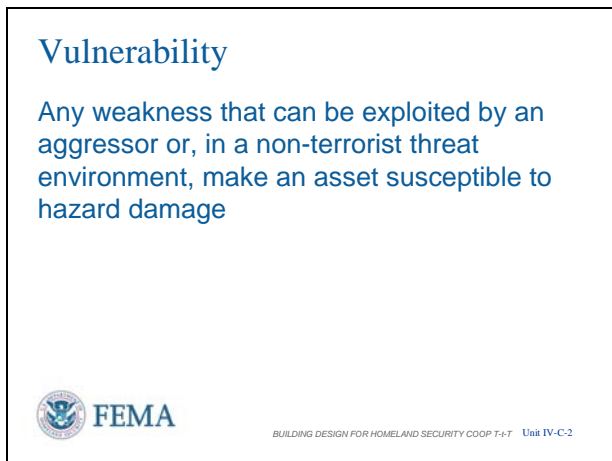


Introduction and Unit Overview

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-C-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-C-3

Unit Objectives


Explain what constitutes a vulnerability.

Identify vulnerabilities using the Building Vulnerability Assessment Checklist.

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.

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



BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IV-C-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-C-4

Vulnerability Assessment

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



BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IV-C-4

Vulnerability Assessment in this context has three components:

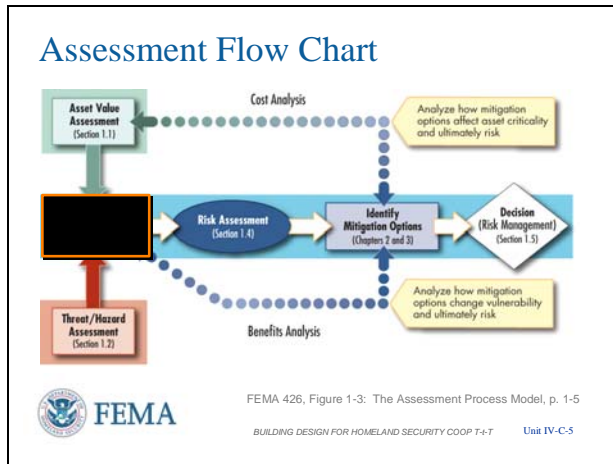
- Identify site and building systems design issues
- Evaluate design issues against type and level of threat
- Determine level of protection sought for each mitigation measure against each threat

[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

VISUAL IV-C-5



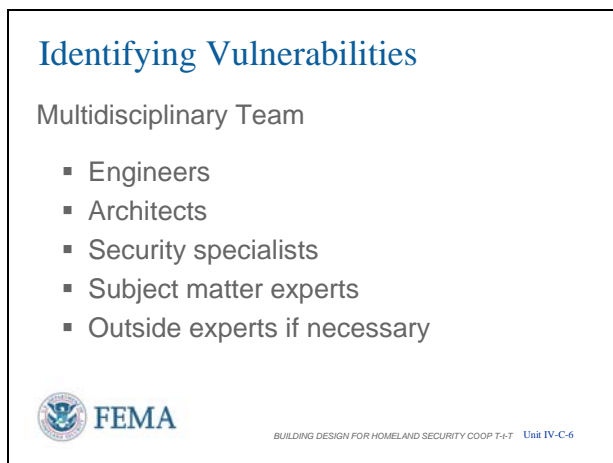
Assessment Flow Chart

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-C-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

VISUAL IV-C-7

Vulnerability Assessment Preparation

Coordinate with the building stakeholders:

- Site and Building Plans
- Utilities
- Emergency Plans (shelter, evacuation)
- Interview schedules
- Escorts for building access



BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IV-C-7

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.

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:

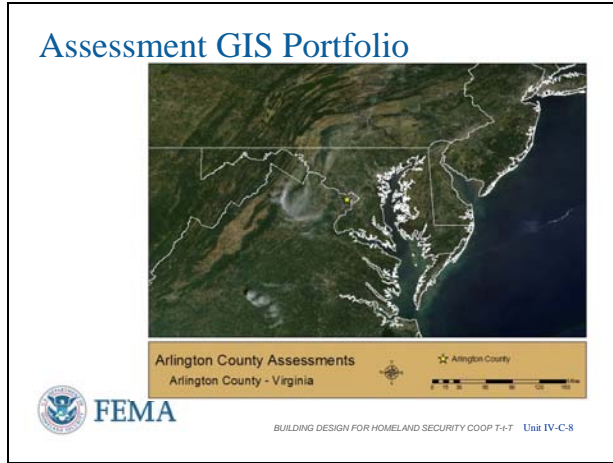
- Site and Building Plans
- Utilities
- Emergency Plans (shelter, evacuation)
- Interview schedules [ensure the people who can answer the team assessment questions are available]
- Escorts for building access

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.

COOP: The vulnerability assessment process also works well when evaluating an alternate facility. Many questions are consistent between the two processes.

VISUAL IV-C-8



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

Another important resource out of the Geospatial One-Stop initiative is www.geodata.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

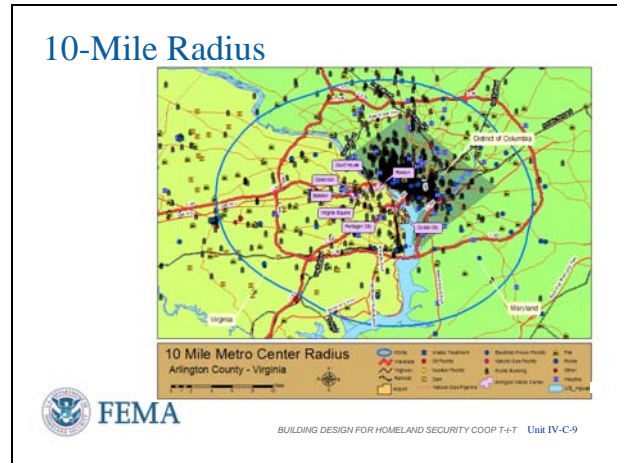
The data sets are a combination of commercial and government (FEMA – HAZUS-MH, US Geologic Survey, state, and local data) imagery interpretation, as well as open source transportation, utility, flood plains, and political boundaries.

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.

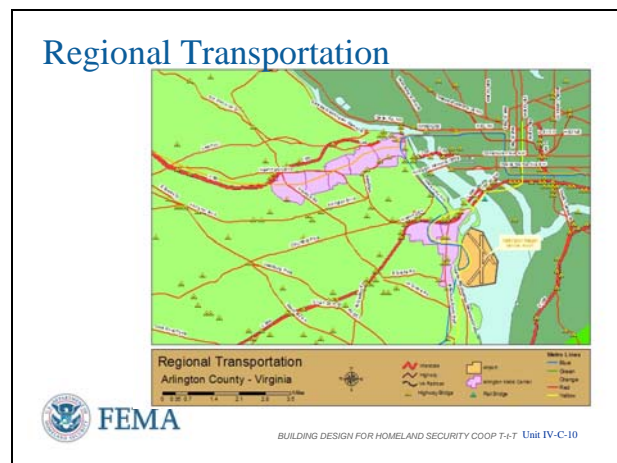
VISUAL IV-C-9



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.

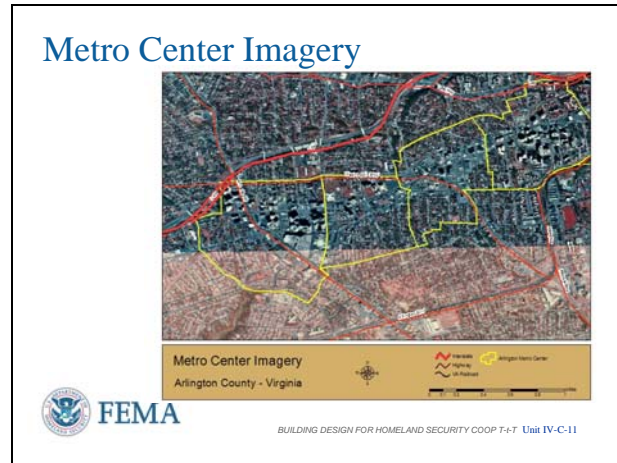
VISUAL IV-C-10



Regional Transportation

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

VISUAL IV-C-11



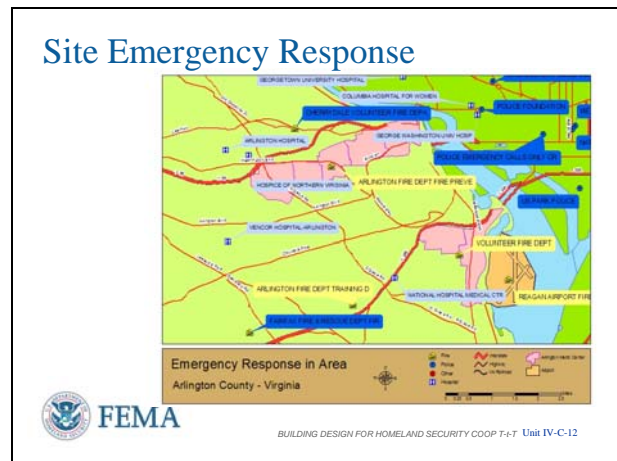
Metro Center Imagery

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.

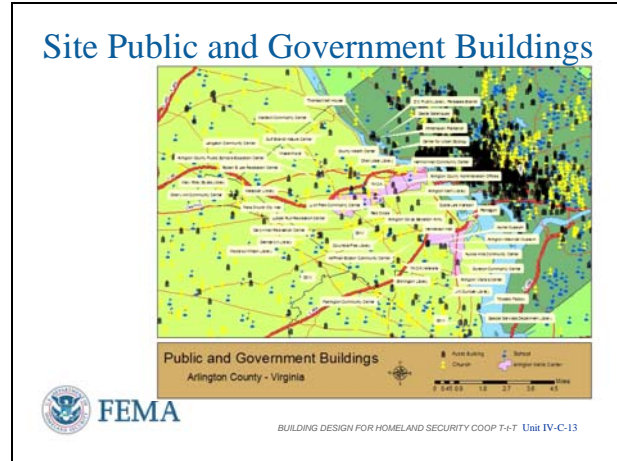
VISUAL IV-C-12



Site Emergency Response

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

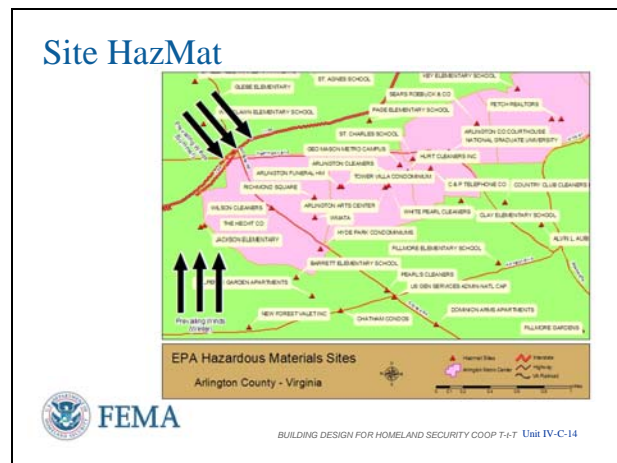
VISUAL IV-C-13



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-C-14

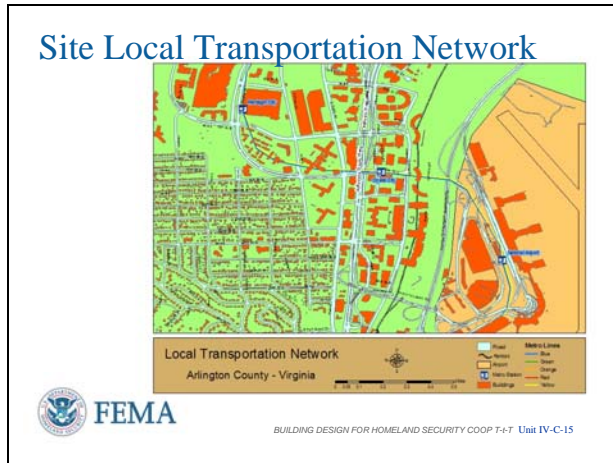


Site HazMat

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.

VISUAL IV-C-15



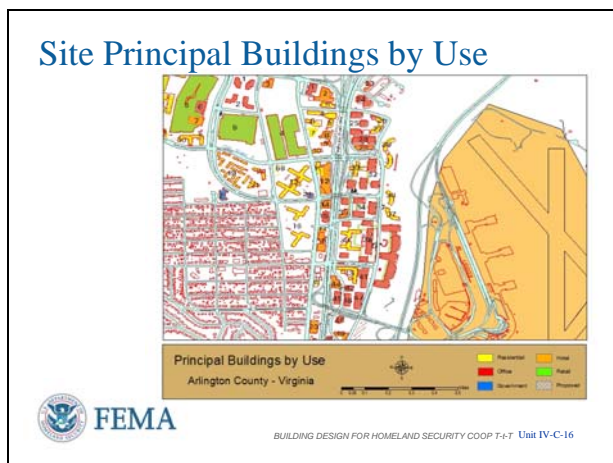
Site Local Transportation Network

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 an emergency.

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

VISUAL IV-C-16

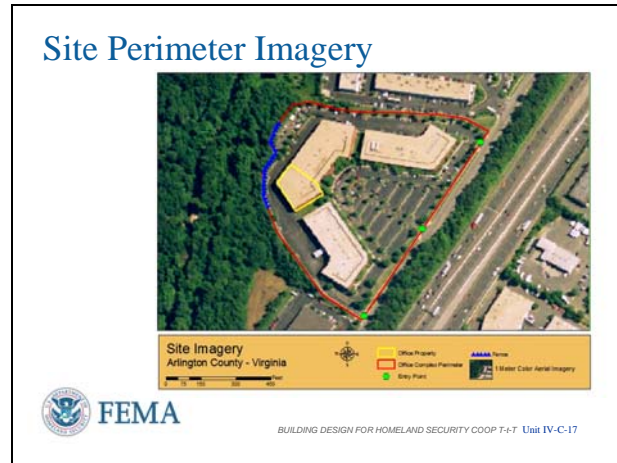


Site Principal Buildings by Use

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.

VISUAL IV-C-17

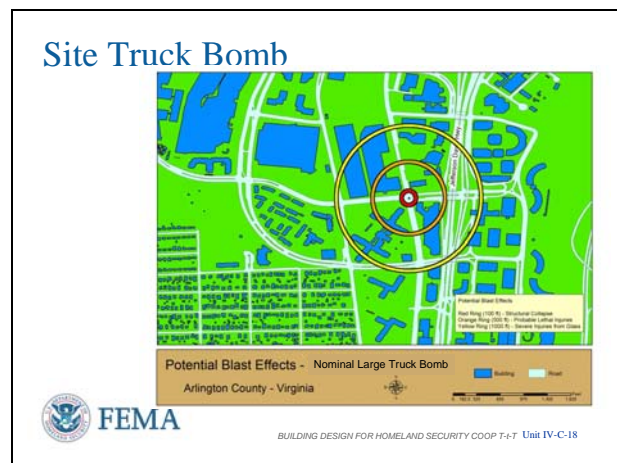


Site Perimeter Imagery

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-C-18

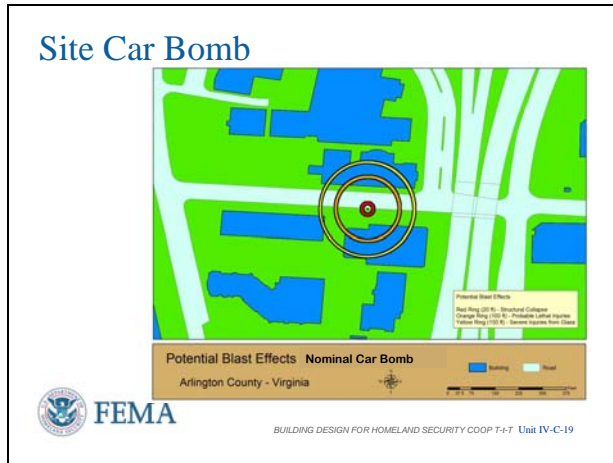


Site Truck Bomb

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.

VISUAL IV-C-19

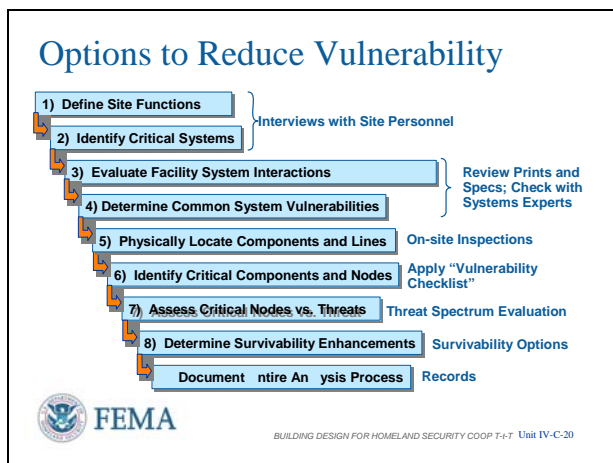


Site Car Bomb

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-C-20



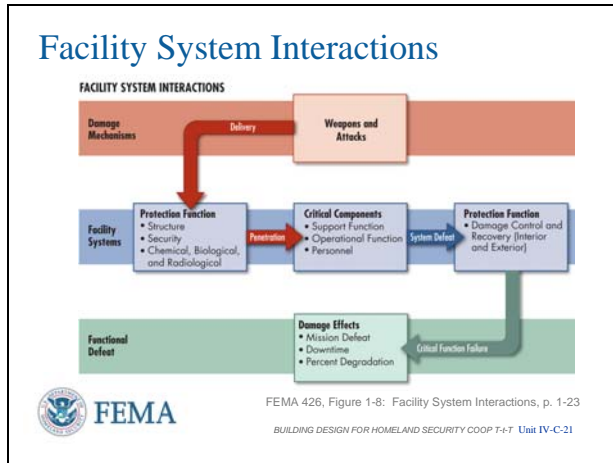
Options to Reduce Vulnerability

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.

VISUAL IV-C-21



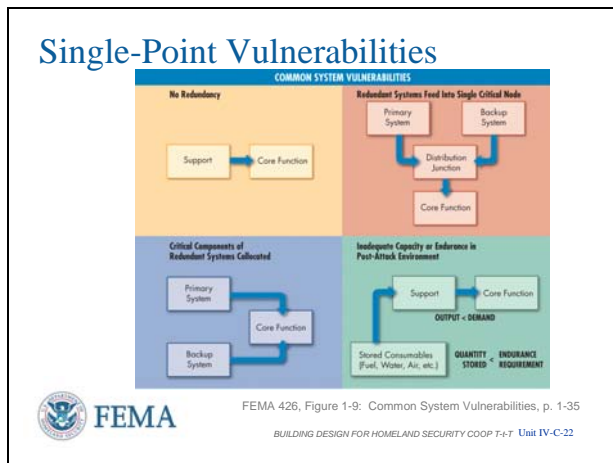
Facility System Interactions

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.

VISUAL IV-C-22



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.

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.

COOP: SPVs are equally important to the continued functioning of alternate facilities.

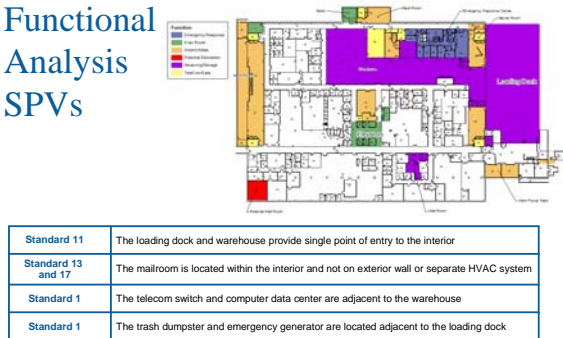
Identification and protection of these Single-Point Vulnerabilities is a key aspect of the assessment process.

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

VISUAL IV-C-23

Functional Analysis SPVs



Standard 11	The loading dock and warehouse provide single point of entry to the interior
Standard 13 and 17	The mailroom is located within the interior and not on exterior wall or separate HVAC system
Standard 1	The telecom switch and computer data center are adjacent to the warehouse
Standard 1	The trash dumpster and emergency generator are located adjacent to the loading dock

FEMA 426, Figure 1-10: Non-Redundant Critical Functions Collocated Near Loading Dock, p. 1-41
BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IV-C-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-C-24

Infrastructure SPVs



Air Intakes Drive Through Electrical Service Telecom Service

FEMA 426, Figure 1-11: Vulnerability Examples, p. 1-42
BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IV-C-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.

COOP: Again, these SPVs are concerns at alternate facilities whether from natural or man-made hazards.

VISUAL IV-C-25

Building Vulnerability Assessment Checklist

- Compiles best practices from many sources
- Includes questions that determine if critical systems will continue to function during an emergency or threat event
- Organized into 13 sections
 - Each section should be assigned to a knowledgeable individual
 - Results of all sections should be integrated into a master vulnerability assessment
 - Compatible with CSI Master Format standard to facilitate cost estimates



BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IV-C-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.

COOP: These checklist questions have been cross-referenced in the Risk Management Database (Unit 6) to FPC-65 requirements with some 10 questions identified as COOP specific and covered separately.


INSTRUCTOR NOTES

CONTENT/ACTIVITY

VISUAL IV-C-26

Building Vulnerability Assessment Checklist

Site	Electrical Systems
Architectural	Fire Alarm Systems
Structural Systems	Communications and IT Systems
Building Envelope	Equipment Operations and Maintenance
Utility Systems	Security Systems
Mechanical Systems (HVAC and CBR)	Security Master Plan
Plumbing and Gas Systems	



BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IV-C-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-C-27

Building Vulnerability Assessment Checklist

Vulnerability Question	Guidance	Observations
6 Mechanical Systems (HVAC and CBR)		
6.1 Where are the air intakes and exhaust louvers for the building? (low, high, or midpoint of the building structure) Are the intakes and exhausts accessible to the public?	Air intakes should be located on the roof or as high as possible. Otherwise secure with CPIED-compliant fencing or enclosure. The fencing or enclosure should have a sloped roof to prevent throwing anything into the enclosure near the intakes. Ref: CDC/NIOSH Pub 2002-139	
6.2 Is roof access limited to authorized personnel by means of locking mechanisms? Is access to mechanical areas similarly controlled?	Roofs are like entrances to the building and are like mechanical rooms when HVAC is installed. Adjacent structures or landscaping should not allow access to the roof. Ref: GSA PBS -P100, CDC/NIOSH Pub 2002-139, and LBNL Pub 51959	



FEMA 426, Adapted from Table 1-22: Building Vulnerability Assessment Checklist, p. 1-46 to 1-92
BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IV-C-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.

VISUAL IV-C-28

Building Vulnerability Assessment Checklist



1.15	Is there minimum setback distance between the building and parked cars?
4.1	What is the designed or estimated protection level of the exterior walls against the postulated explosive threat?
4.2	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.)?



FEMA 426, Adapted from Table 1-22: Building Vulnerability Assessment Checklist, p. 1-46 to 1-92
BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IV-C-28

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.

VISUAL IV-C-29

Building Vulnerability Assessment Checklist



2.19	Are loading docks and receiving and shipping areas separated in any direction from utility rooms, utility mains, and service entrances, including electrical, telephone/data, fire detection/alarm systems, fire suppression water mains, cooling and heating mains, etc.?
1.16	Does adjacent surface parking on site maintain a minimum stand-off distance? 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-P100



FEMA 426, Adapted from Table 1-22: Building Vulnerability Assessment Checklist, p. 1-46 to 1-92
BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IV-C-29


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.

VISUAL IV-C-30

Building Vulnerability Assessment Checklist



6.1	Where are the air intakes and exhaust louvers for the building? (low, high, or midpoint of the building structure) Are the intakes and exhausts accessible to the public?
1.9	Is there any potential access to the site or building through utility paths or water runoff? (Eliminate potential site access through utility tunnels, corridors, manholes, storm water runoff culverts, etc. Ensure covers to these access points are secured.)
3.1	What type of construction? What type of concrete and reinforcing steel? What type of steel? What type of foundation?

FEMA 426, Adapted from Table 1-22: Building Vulnerability Assessment Checklist, p. 1-46 to 1-92
BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IV-C-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-C-31

Building Vulnerability Assessment Checklist



5.19	By what means does the main telephone and data communications interface the site or building?
5.20	Are there multiple or redundant locations for the telephone and communication service? Does the fire alarm system require communication with external sources?
5.21	By what method is the alarm signal sent to the responding agency: telephone, radio, etc.? Is there an intermediary alarm monitoring center?

FEMA 426, Adapted from Table 1-22: Building Vulnerability Assessment Checklist, p. 1-46 to 1-92
BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IV-C-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.

VISUAL IV-C-32

Vulnerability Rating

Criteria		
Very High	10	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 the entire building would be only functional again after a very long period of time after the attack.
High	8-9	High – One or more major 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 would be only functional again after a long period of time after the attack.
Medium High	7	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 most critical functions would be only operational again after a long period of time after the attack.

Key elements

- Number of weaknesses
- Aggressor potential accessibility
- Level of redundancies/physical protection
- Time frame for building to become operational again

FEMA 452, Table 3-4: Vulnerability Rating, p. 3-16
 BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IV-C-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.

VISUAL IV-C-33

Vulnerability Rating (continued)

Criteria		
Medium	5-6	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 most part of the building would be only functional again after a considerable period of time after the attack.
Medium Low	4	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 most critical functions would be only operational again after a considerable period of time after the attack.
Low	2-3	Low – A minor weakness has been identified that slightly increases the susceptibility of the asset to an aggressor or hazard. The building has incorporated a good level of redundancies/physical protection and the building would be operational within a short period of time after an attack.
Very Low	1	Very Low – No weaknesses exist. The building has incorporated excellent redundancies/physical protection and the building would be operational immediately after an attack.

Key elements

- Number of weaknesses
- Aggressor potential accessibility
- Level of redundancies /physical protection
- Time frame for building to become operational again

FEMA 452, Table 3-4: Vulnerability Rating, p. 3-16
BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IV-C-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.

VISUAL IV-C-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 426, Adaptation of Table 1-20: Site Functional Pre-Assessment Screening Matrix, p. 1-38
BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IV-C-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-C-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 426, Adaptation of Table 1-21: Site Infrastructure Systems Pre-Assessment Screening Matrix, p. 1-39
BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IV-C-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

VISUAL IV-C-36

Summary

Step-by-Step Analysis Process:

- Expertly performed by experienced personnel
- Determines critical systems
- Identifies vulnerabilities
- Focuses survivability mitigation measures on critical areas
- Essential component of Critical Functions and Critical Infrastructure Matrices



BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IV-C-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-C-37

Vulnerability Rating Considerations

Go to Page SM IV-C-2 in your Student Manual

1. Effectiveness of threat tactic / hazard against asset
2. Redundancy
3. Layers of Defense and depth of layers
4. Cyber



BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IV-C-37

Vulnerability Rating Considerations

As a further emphasis to ensure understanding of definitions, a review of Vulnerability and how it can be looked at is provided here. The list on the slide is expanded with examples on the designated page of the Student Manual. [It is also the first page of the Case Study Activity later in this document (about 3 pages).]

Walk the students through each point on the slide using the expanded information in the Case Study Activity.

VISUAL IV-C-38

Unit IV Case Study Activity

Vulnerability Rating

Background


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

Requirements: Vulnerability Rating Approach

Use rating scale of 1 (very low or no weakness) to 10 (one or major weaknesses)

Refer to Case Study and rate the vulnerability of asset-threat/hazard pairs:

- Critical Functions
- Critical Infrastructure



BUILDING DESIGN FOR HOMELAND SECURITY COOP T-t-T Unit IV-C-38

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).

NOTE to instructor: Work tables and room to draw out student answers, especially when they are different from the “school solution.” Point out that team consistency of rationale as applied to all assets is more important than the specific number provided in the rating.

Keep in mind that there are no incorrect answers. It is more important to be able to clearly explain and support the underlying rationale for the values that have been assigned. Also it has been proven that 7 people working effectively as a group can achieve genius level in their consensus response.

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.*

Activity Requirements:

NOTE to instructor: Walk the students through the completed examples so that they have a feel for the ultimate goal of this activity.

- Working with your team, review Critical Function vulnerability ratings and provide rationale for the ratings as given or adjusted. For Critical Infrastructure review ratings given, provide vulnerability ratings where not given, and provide rationale for the ratings.
- Transfer your team answers to the Risk Matrix poster.

Take 35 minutes to complete this part of the

INSTRUCTOR NOTES

CONTENT/ACTIVITY

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 (C) CASE STUDY ACTIVITY:
VULNERABILITY RATINGS
(COOP Version)**

Vulnerability Rating Considerations (susceptibility to damage resulting from that attack tactic being used against that asset or hazard occurring that affects that asset)

1. Effectiveness of threat tactic / hazard against asset
 - The greater the predicted or modeled effectiveness the greater the vulnerability
 - Number of people injured or killed
 - Amount of building destroyed
 - Level of publicity expected to occur

2. Redundancy
 - Back-up facility or equipment that offsets the loss of the asset
 - Partial back-up: 10 to 90%
 - One full back-up: 100%
 - Additional back-up depending upon workload: 125%, 150%, 200%
 - The greater the redundancy the less the vulnerability; but too much redundancy can reduce reliability

3. Layers of Defense and depth of layers
 - DENY measures as defined on page 1-9 of FEMA 426 are methods of hardening the site and building and would be described better as mitigation of vulnerability
 - How far do the mitigation measures keep the threat away from the asset?
 - The more complete the Layers of Defense and the greater the depth (stand-off distance) of these layers the lower the vulnerability.

4. Cyber
 - Can a terrorist or hacker get any access to the function or infrastructure that has components of electronics, software, data (information technology), or communications
 - If none of these components, the vulnerability is very low
 - If components are all stand alone, the vulnerability is also very low, but probably greater than one
 - Example: electric typewriters give off varying radio frequencies during operation that allows specific key strokes to be identified and, therefore, recreated
 - If components use wireless, radio frequency, cell phones, land lines, or hard-wired internet or communications connections then vulnerability is based upon DETECT (anti-virus or access attempts), DETER (access protocols, physical security), DENY (firewalls, encryption, shielding), or other measures
 - Cyber experts have detailed and in-depth approaches to assessing vulnerability. A proposed industry standard is CVSS (Common Vulnerability Scoring System) which prioritizes vulnerabilities and indicates to system administrators the tasks they should expend available manpower upon.

**UNIT IV (C) CASE STUDY ACTIVITY:
VULNERABILITY RATINGS
(COOP 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.

Vulnerability Rating Activities

1. Complete the tables for Critical Functions and Critical Infrastructure Vulnerability Ratings.
 - Some ratings and rationale are provided as **examples**.
 - Adjust ratings as desired by team consensus and provide rationale for the provided or adjusted ratings as appropriate.
 - Refer to the Appendix C Case Study as needed.
2. Transfer the vulnerability ratings to the Risk Matrix poster after reaching team consensus on the answers.

CI/BC Critical Functions Vulnerability Ratings

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

RATIONALE

Cyber Attack is based upon the level of interaction the function has with the internet or other communications systems.

High End: Do not expect much vulnerability at this level. CI/BC is an Information Company whose business it is to ensure security of its systems and products.

A variety of firewalls and other security systems are in place to protect the company and its clients. The firewall solution is based on the Cisco PIX to provide highly resilient firewall protection. Other security systems include reporting and analysis tools and network detection devices, which help protect the company’s computers from hacking.

If Engineering/IT Technicians included building operations and maintenance personnel whose systems are accessible from home through passwords and firewalls to monitor and adjust parameters of concern, this would be a high end vulnerability due to the current configuration of such software. This was not included in the Case Study, therefore, not given a high vulnerability rating.

Communications set at the high end due to wireless networks that are less secure than wired networks and are more accessible to the terrorist.

Middle: Administration, Engineering/IT Technicians, and Security are mid-range rated due to the use of systems connected to the internet that are required for their daily operations, but the level of mitigation capability is not as great as would be found in the Data Center.

Low End: While not explained in the Case Study, the Loading Dock/Warehouse and Housekeeping are expected to have very little or no interaction with the internet or communications systems per se. Their main interaction may be through cell phone communications. The Loading Dock / Warehouse may have an internet link to identify dates, times, and access information for deliveries or for purchasing / warehousing items.

The Data Center is also on the low end due to the security explanation given under High End above.

Armed Attack *is based upon the normal work location and accessibility to that location to employ this tactic. Note that all Functions will have vulnerability while transiting to and from work, but that is not considered here.*

High End: *Administration and Loading Dock are relatively high as they are on the exterior envelope and readily accessible – window area in front for Administration, and rear for Loading Dock. The Loading Dock could be rated a little lower since it is not always observable like Administration personnel at the windows.*

Middle: *Engineering / IT Technicians will normally be found throughout the building, but least likely near the exterior envelope. They will many times be behind additional security access controls.*

Security is also given a mid-range rating as they are readily identifiable personnel and have greater target value to the terrorist.

Low End: *The Data Center and Communications are behind another layer of protection behind the Administration area on the first floor, thus, are less vulnerable than Administration as a whole.*

Housekeeping may come at a specific time each day, but moves throughout the building and is in the building only a short time. If arrival is at the same time, then Housekeeping will have greater vulnerability.

Vehicle Bomb *demonstrates the indiscriminate nature of this tactic which has a global effect on the whole building as the building is relatively small and a Design Basis Threat bomb will impact a good portion of the building.*

High End: *All functions are vulnerable to a vehicle bomb due to lack of stand-off distance, especially at the rear of the building and the construction of the building. In one way or another all functions will be affected by a vehicle bomb. Vulnerability Ratings of 9 or 10 would also be justifiable.*

Middle:

Low End:

CBR Attack is also a global effect upon the building, with variation based upon location within the building, HVAC system configuration, and the tightness of the exterior envelope and internal areas.. In this case there is a single HVAC system with no mitigation measures installed, a ground level air intake and a roll-up door on the Loading Dock.

High End: *As with Vehicle Bomb, a high end rating is appropriate as there are no mitigation measures. Vulnerability Ratings of 9 or 10 would also be justifiable.*

Middle:

Low End:

CI/BC Critical Infrastructure Vulnerability Ratings

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

RATIONALE

Cyber Attack is based upon connectivity to the internet and communications systems.

High End: None at this level of vulnerability as would be expected for an Information Company.

Middle: Utility Systems, Mechanical Systems, and Electrical Systems are mid-range vulnerability. Utility Systems coming to the Site are controlled by their respective companies and have more points of attack than the CI/BC building, especially if using legacy SCADA (Supervisory Control and Data Acquisition) systems. Internal building mechanical and electrical systems have various levels of computer controls and access to internet. Without specific information, a rating of 5 allows an average estimate of vulnerability until further assessment can be made.

IT/Communications Systems show a balance of the protection this Information Company has put into its Information Technology systems and the vulnerability of wireless communications that also come under this heading. If there are a great number of

wireless networks, then this vulnerability rating should be increased. Since these systems have the greatest connectivity to the internet and to communications, it is logical that it should get the highest vulnerability rating.

Low End: *Site, Architectural, Structural Systems, and Envelope Systems are not expected to have any connections to the internet or communications and this is confirmed in the Case Study. Plumbing and Gas Systems are also normally not connected to the internet or communications. The Fire Alarm System is slightly higher in vulnerability rating as the system is hard wired to the local fire department.*

If access control is at the Site perimeter and if it is connected to internet or communications then the vulnerability rating of Site would be much higher.

Armed Attack *follows the same logic as critical functions and this tactic – normal location and accessibility to that location.*

High End: *As with the Functions; Site, Architectural, Structural Systems, and Envelope Systems have a high vulnerability to this tactic as they are readily accessible and observable from a distance with limited mitigation measures, such as roving security patrols.*

Middle: *Utility Systems are given a middle vulnerability rating from two aspects: 1) all utilities are underground so that they have little vulnerability to armed attack and 2) some utility components are readily identifiable, readily accessible, and observable in the rear of the building – electric power transformer, backup generator, and gas metering which are all vulnerable to this tactic.*

Similarly Mechanical Systems are given a mid-range rating as the critical cooling towers associated with the HVAC system are exposed, readily identifiable, and accessible to this tactic.

Low End: *The remaining systems – Plumbing and Gas, Electrical, Fire Alarm, and IT/Communications are all internal to the building, not readily identifiable from the outside, and are behind layers of access control that reduce their vulnerability to armed attack.*

Vehicle Bomb *exhibits its global effects nature with proximity to the bomb raising the vulnerability rating.*

High End: *Due to the lack of stand-off, lack of hardening, and the Design Basis Threat being considered, a high end rating is applicable for all infrastructure that is above ground and, therefore, will be impacted by air blast, fragmentation, and breaching effects. Vulnerability Ratings of 9 or 10 would also be justifiable.*

Middle: *The one variance in this tactic is Utility Systems. Since all these life lines (piping / cabling) are underground, their vulnerability to a vehicle bomb is greatly reduced. The utility life line would have to be right under the bomb so that the crater would cut or compress the life line. Also, the components above ground are less susceptible to bomb blast than armed attack due to the nature of their construction.*

Low End:

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.

High End: As with Vehicle Bomb, a high end rating is appropriate for Site as there are no mitigation measures for a CBR attack. Vulnerability Ratings of 9 or 10 would also be justifiable. This tactic will deny access to the building and its critical functions and critical infrastructure based upon the type and persistency of agent.

Likewise, the Mechanical Systems have no mitigation measures in place, specifically HVAC, warranting a high rating. As the IT/Communication Systems require 24/7 attention and they are linked to the HVAC system, IT/Comms warrants a high rating as their operation can be severely impacted during and after a CBR attack.

Middle:

Low End: Low end vulnerability rating is given to Architectural, Structural Systems, and Envelope Systems as the CBR attack will have little to no effect upon these systems performing their functions. Decontamination will be the main response.

Utility Systems will also continue to function properly during and after a CBR attack, but these systems may require maintenance access which will be hampered by the persistency of any agents. Thus, a higher vulnerability rating is warranted.

Similarly, Plumbing and Gas Systems, Electrical Systems, Fire Alarm Systems will generally continue to operate during and after a CBR attack. Maintenance can be delayed until decontamination is complete.