Unit IV
Vulnerability Assessment
Vulnerability

Any weakness that can be exploited by an aggressor or, in a non-terrorist threat environment, make an asset susceptible to hazard damage
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.
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
Assessment Flow Chart

1. **Asset Value Assessment (Section 1.1)**
2. **Vulnerability Assessment (Section 1.3)**
3. **Threat/Hazard Assessment (Section 1.2)**
4. **Risk Assessment (Section 1.4)**
5. **Identify Mitigation Options (Chapters 2 and 3)**
6. **Decision (Risk Management) (Section 1.5)**

**Flowchart Descriptions**
- **Asset Value Assessment**: Analyze how mitigation options affect asset criticality and ultimately risk.
- **Vulnerability Assessment**: Analyze how mitigation options change vulnerability and ultimately risk.
- **Risk Assessment**: Cost Analysis
- **Identify Mitigation Options**: Benefits Analysis
- **Decision**: Analyze how mitigation options change vulnerability and ultimately risk.

**FEMA**

**BUILDING DESIGN FOR HOMELAND SECURITY**
Identifying Vulnerabilities

Multidisciplinary Team

- Engineers
- Architects
- Security specialists
- Subject matter experts
- Outside experts if necessary
Vulnerability Assessment Preparation

Coordinate with the building stakeholders:

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

Arlington County Assessments
Arlington County - Virginia
10-Mile Radius
Regional Transportation

Arlington County - Virginia

FEMA
BUILDING DESIGN FOR HOMELAND SECURITY  Unit IV-10
Metro Center Imagery

Arlington County - Virginia
Site Emergency Response

Emergency Response in Area
Arlington County - Virginia

FEMA
BUILDING DESIGN FOR HOMELAND SECURITY Unit IV-12
Site Public and Government Buildings

Public and Government Buildings
Arlington County - Virginia

FEMA
Site HazMat

EPA Hazardous Materials Sites
Arlington County - Virginia
Site Local Transportation Network
Site Principal Buildings by Use

Principal Buildings by Use
Arlington County - Virginia
Site Perimeter Imagery
Site Truck Bomb

Potential Blast Effects - 11,000 lbs Truck Bomb

Arlington County - Virginia
Site Car Bomb
Options to Reduce Vulnerability

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 vs. Threats
8) Determine Survivability Enhancements
9) Document Entire Analysis Process

- Interviews with Site Personnel
- Review Prints and Specs; Check with Systems Experts
- On-site Inspections
- Apply “Vulnerability Checklist”
- Threat Spectrum Evaluation
- Survivability Options
- Records
Facility System Interactions

Figure 1-8: Facility System Interactions, page 1-23

BUILDING DESIGN FOR HOMELAND SECURITY

Unit IV-21
Single-Point Vulnerabilities
Function Analysis

SPVs

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

Figure 1-10: Non-Redundant Critical Functions Collocated Near Loading Dock, p. 1-41

BUILDING DESIGN FOR HOMELAND SECURITY Unit IV-23
Infrastructure SPVs

Air Intakes

Drive Through

Electrical Service

Telecom Service

BUILDING DESIGN FOR HOMELAND SECURITY
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 Vulnerability Assessment Checklist

Site
Architectural
Structural Systems
Building Envelope
Utility Systems
Mechanical Systems (HVAC and CBR)
Plumbing and Gas Systems

Electrical Systems
Fire Alarm Systems
Communications and IT Systems
Equipment Operations and Maintenance
Security Systems
Security Master Plan
## Building Vulnerability Assessment Checklist

<table>
<thead>
<tr>
<th>Vulnerability Question</th>
<th>Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mechanical Systems (HVAC and CBR)</strong></td>
<td></td>
</tr>
</tbody>
</table>
| 6.1 Where are the air intakes and exhaust louvers for the building? (low, high, or midpoint of the building structure) | Air intakes should be located on the roof or as high as possible. Otherwise secure within CPTED-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 |
| Are the intakes and exhausts accessible to the public? | |
| 6.2 Is roof access limited to authorized personnel by means of locking mechanisms? | 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 |
| Is access to mechanical areas similarly controlled? | |
### Building Vulnerability Assessment Checklist

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

Extracted from Table 1-22: Building Vulnerability Assessment Checklist, pages 1-46 to 1-92.
## Building Vulnerability Assessment Checklist

<table>
<thead>
<tr>
<th>1.15</th>
<th>Is there minimum setback distance between the building and parked cars?</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>What is the designed or estimated protection level of the exterior walls against the postulated explosive threat?</td>
</tr>
<tr>
<td>4.2</td>
<td>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.)?</td>
</tr>
</tbody>
</table>
What type of construction?

What type of concrete and reinforcing steel?

What type of steel?

What type of foundation?

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.)

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?
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 standoff 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*
Vulnerability Rating

**Very High** – One or more major weaknesses have been identified that make the asset extremely susceptible to an aggressor or hazard.

**High** - One or more significant weaknesses have been identified that make the asset highly susceptible to an aggressor or hazard.

**Medium High** – An important weakness has been identified that makes the asset very susceptible to an aggressor or hazard.

**Medium** – A weakness has been identified that makes the asset fairly susceptible to an aggressor or hazard.

**Medium Low** – A weakness has been identified that makes the asset somewhat susceptible to an aggressor or hazard.

**Low** – A minor weakness has been identified that slightly increases the susceptibility of the asset to an aggressor or hazard.

**Very Low** – No weaknesses exist.
### Critical Functions

<table>
<thead>
<tr>
<th>Function</th>
<th>Cyber attack</th>
<th>Armed attack (single gunman)</th>
<th>Vehicle bomb</th>
<th>CBR attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Value</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Threat Rating</td>
<td>8</td>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Vulnerability Rating</td>
<td>7</td>
<td>7</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>Engineering</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Value</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Threat Rating</td>
<td>8</td>
<td>5</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>Vulnerability Rating</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>9</td>
</tr>
</tbody>
</table>

Extracted from Table 1-20, page 1-38
## Critical Infrastructure

<table>
<thead>
<tr>
<th>Function</th>
<th>Cyber attack</th>
<th>Armed attack (single gunman)</th>
<th>Vehicle bomb</th>
<th>CBR attack</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Site</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Value</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Threat Rating</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Vulnerability Rating</td>
<td>3</td>
<td>5</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td><strong>Structural Systems</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Value</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Threat Rating</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Vulnerability Rating</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>9</td>
</tr>
</tbody>
</table>

Extracted from Table 1-21, page 1-39
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 Infrastructure and Critical Function Matrices
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 HIC case study and rate the vulnerability of asset-threat/hazard pairs:

- HIC Critical Functions
- HIC Infrastructure