



Risk Management Series

# Building Design for Homeland Security

Student Manual

January 2004



FEMA

**RISK MANAGEMENT SERIES**

Building Design for  
Homeland Security

**PROVIDING PROTECTION TO PEOPLE AND BUILDINGS**

*Student Manual*



**FEMA**

[www.fema.gov](http://www.fema.gov)

---

Any opinions, findings, conclusions, or recommendations expressed in this publication do not necessarily reflect the views of FEMA. Additionally, neither FEMA or any of its employees makes any warrantee, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process included in this publication. Users of information from this publication assume all liability arising from such use.

# BACKGROUND AND ACKNOWLEDGMENTS

---

## BACKGROUND

The Federal Emergency Management Agency (FEMA) developed the *Building Design for Homeland Security Course (E155)*, to provide needed information on how to mitigate the effects of potential terrorist attacks.

The purpose of E155 is to familiarize students with assessment methodologies available to identify the relative level of risk for various threats, including blast and chemical, biological, or radiological. The students will be introduced to FEMA 426 and will be asked to provide cost-effective mitigation measures for a range of manmade hazards. The primary target audience for this course includes engineers, architects, and building officials.

## ACKNOWLEDGMENTS

### Principal Authors:

Michael Chipley, UTD, Inc.

Michael Kaminskas, UTD, Inc.

### Contributors:

Milagros Kennett, FEMA, Project Officer, Risk Management Series Publications

Dan Bondroff, EMI Training Specialist

Eric Letvin, Greenhorne & O'Mara, Inc., Consultant  
Project Manager

Christopher Arnold, Building Systems Development, Inc.

Dwight Johnson, All About Training Instruction System  
Designer

Gina Wightman, All About Training Instruction System  
Designer

Deb Daly, Greenhorne & O'Mara, Inc.

Wanda Rizer, Greenhorne & O'Mara, Inc.

Julie Liptak, Greenhorne & O'Mara, Inc.

This course was prepared under contract to FEMA. It will be revised periodically, and comments and feedback to improve future editions are welcome. Please send comments and feedback by e-mail to [riskmanagementseriespubs@dhs.gov](mailto:riskmanagementseriespubs@dhs.gov)



## AGENDA

### **Day 1**

### **Instructor**

8:30 a.m.	Unit I – Introduction and Course Overview	Michael Chipley, Ph.D.
10:00 a.m.	Break	Eric Letvin, Esq.
10:15 a.m.	Unit II – Asset Value Assessment	Eric Letvin, Esq.
11:30 a.m.	Lunch	Eric Letvin, Esq.
12:30 p.m.	Unit III – Threat/Hazard Assessment	Michael Chipley, Ph.D.
1:45 p.m.	Break	Eric Letvin, Esq.
2:00 p.m.	Unit IV – Vulnerability Assessment	Michael Kaminskas, P.E.
3:45 p.m.	Break	Eric Letvin, Esq.
4:00 p.m.	Unit V – Risk Assessment/Risk Management	Eric Letvin, Esq.
4:45 p.m.	Day 1 Wrap-up and Day 2 Forecast	Eric Letvin, Esq.
5:00 p.m.	Dinner	Eric Letvin, Esq.

---



## AGENDA

### Day 2

### **Instructor**

8:30 a.m.	Day 1 Review and Day 2 Overview	Eric Letvin, Esq.
8:45 a.m.	Unit V – Risk Assessment/Risk Management (continued)	Michael Chipley, Ph.D.
9:15 a.m.	Unit VI – Explosive Blast	Michael Kaminskas, P.E.
10:15 a.m.	Break	Eric Letvin, Esq.
10:30 a.m.	Unit VII – Chemical, Biological, and Radiological Measures	Michael Chipley, Ph.D.
11:30 a.m.	Lunch	Eric Letvin, Esq.
12:30 p.m.	Written Exam	Michael Chipley, Ph.D. Michael Kaminskas, P.E.
1:00 p.m.	Written Exam Review	Michael Chipley, Ph.D. Michael Kaminskas, P.E.
1:30 p.m.	Break	Eric Letvin, Esq.
1:45 p.m.	Unit VIII – Site and Layout Design Guidance	Chris Arnold, FAIA
3:30 p.m.	Break	Eric Letvin, Esq.
3:45 p.m.	Unit VIII – Site and Layout Design Guidance (continued)	Chris Arnold, FAIA
4:30 p.m.	Day 2 Wrap-up and Day 3 Forecast	Eric Letvin, Esq.
5:00 p.m.	Dinner	Eric Letvin, Esq.

---

---



## AGENDA

### **Day 3**

### **Instructor**

8:30 a.m.	Day 2 Review and Day 3 Overview	Eric Letvin, Esq.
8:45 a.m.	Unit IX – Building Design Guidance	Michael Kaminskas, P.E.
10:15 a.m.	Break	Eric Letvin, Esq.
10:30 a.m.	Unit IX – Building Design Guidance (continued)	Michael Kaminskas, P.E.
11:30 a.m.	Lunch	Eric Letvin, Esq.
12:30 p.m.	Unit X – Electronic Security Systems	Eric Letvin, Esq.
1:15 p.m.	Break	Eric Letvin, Esq.
1:30 p.m.	Unit XI – Finalization of Case Study Results [Goal is to brief building owner on prioritized recommendations and justifications for security work.]	Michael Chipley, Ph.D. Michael Kaminskas, P.E.
2:15 p.m.	Break	Eric Letvin, Esq.
2:30 p.m.	Unit XI – Presentation of Group Case Study Results and Discussion (continued) [Assumes 6 teams and 10 minutes per team to present and 5 minutes per team to discuss.]	Michael Chipley, Ph.D. Michael Kaminskas, P.E.
4:00 p.m.	Unit XII – Course Wrap-up	Eric Letvin, Esq.
5:00 p.m.	Adjourn	Eric Letvin, Esq.

---

---

# Unit I

---

**COURSE TITLE**

Building Design for Homeland Security

---

**UNIT TITLE**

Introduction and Course Overview

---

**OBJECTIVES**

1. Describe the goal, objectives, and agenda for the course
  2. Describe and find material in the course reference manual and student activity handout
- 

**SCOPE**

This unit will cover the following topics:

1. Welcome and Opening Remarks
  2. Instructor Introductions
  3. Administrative Information
  4. Student Introductions
  5. Course Overview
  6. Course Materials
  7. Activity: Become familiar with Case Study materials
- 

**REFERENCES**

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*
2. Case Study, Hazardville Information Company (HIC)

---

**This page intentionally left blank**

**UNIT I CASE STUDY ACTIVITY:  
HAZARDVILLE INFORMATION COMPANY (HIC)  
CASE STUDY OVERVIEW**

**Requirements**

Turn to the Appendix A Case Study materials in the Student Manual and briefly peruse the document. Read the “familiarization” questions on the following worksheet, and as a group, complete the worksheet. Use only the Case Study data to answer worksheet questions. Information has been limited in an effort to focus the activity.

<b>Question</b>	<b>Answer</b>	<b>Page # in Case Study</b>
1. What are the major transportation nodes in the surrounding area?	A major interstate highway is located within ¼ mile of the HIC Headquarters.  CSX Transportation and Norfolk-Southern Railway maintain a transportation corridor about ½ mile from HIC. There appear to be no restrictions on the material carried along these rail lines.  Two airports are in the vicinity of HIC. One is a major international airport approximately 8 miles away. The other is a small, but busy general aviation airport approximately 2 miles away.	A-3, A-28 – A-30

<b>Question</b>	<b>Answer</b>	<b>Page # in Case Study</b>
2. What life safety assets are available, and what are their response times?		A-16, A-17, A-27
3. Who are the building's primary occupants and visitors?		A-1, A-2

<b>Question</b>	<b>Answer</b>	<b>Page # in Case Study</b>
4. What hazards may affect HIC?		A-5, A-6, A-28 – A-30
5. What are the prevalent weather/wind conditions at HIC?		A-6
6. What are the critical functions of HIC?		A-21 – 24

<b>Question</b>	<b>Answer</b>	<b>Page # in Case Study</b>
7. What are the components of HIC's critical utility infrastructure?		A-12 – A-19
8. What are the components of HIC's critical building infrastructure?		A-11, A-12, A-16

**Course Title: Building Design for Homeland Security**

Unit I: Introduction and Course Overview

<b>Question</b>	<b>Answer</b>	<b>Page # in Case Study</b>
9. What personnel are key to the operation of HIC?		A-2

**This page intentionally left blank**

## Unit II

---

**COURSE TITLE**

Building Design for Homeland Security

---

**UNIT TITLE**

Asset Value Assessment

---

**OBJECTIVES**

1. Identify the assets of a building or site that can be affected by a threat or hazard
  2. Explain the components used to determine the value of an asset
  3. Determine the critical assets of a building or site
  4. Provide a numerical rating for the asset and justify the basis for the rating
- 

**SCOPE**

The following topics will be covered in this unit:

1. The core functions and critical infrastructure listed on the threat-vulnerability matrix.
  2. Various approaches to determine asset value – Federal Emergency Management Agency, Department of Defense, Department of Justice, and Veterans Affairs.
  3. A rating scale and how to use it to determine an asset value.
  4. Activity: Identify the assets to consider in the case study and determine the asset value for each asset of interest.
- 

**REFERENCES**

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, pages 1-10 to 1-14
2. Case Study – Hazardville Information Company

---

**This page intentionally left blank**



### Identifying Building Assets and Quantifying Asset Values

Refer to **Table 1-2 in FEMA 426** and use the descriptions of these asset categories in the HIC Case Study. Consider the questions on **page 1-11 in FEMA 426** and rate HIC's assets as:

- Very High (10)
- High (8-9)
- Medium High (7)
- Medium (5-6)
- Medium Low (4)
- Low (2-3)
- Very Low (1)

### HIC Critical Functions Asset Rating

Asset	Value	Numeric Value	Rationale
1. Administrative	Medium Low	4	Redundancy and staff skills that can be replaced. Senior managers and financial systems in the same area make the function a key area to protect. Low to medium economic cost to replace.
2. Engineering/IT Technicians	Medium	5	Staff skills that can be replaced, but require specialized expertise. Key equipment and resources may not be replaceable. High economic cost to replace.
3. Loading Dock/Warehouse			

Asset	Value	Numeric Value	Rationale
4. Data Center			
5. Communications			
6. Security			
7. Housekeeping			

---

**HIC Critical Infrastructure Asset Rating**

<b>Asset</b>	<b>Value</b>	<b>Numeric Value</b>	<b>Rationale</b>
1. Site			
2. Architectural			
3. Structural Systems			
4. Envelope Systems			
5. Utility Systems			

**Course Title: Building Design for Homeland Security**

Unit II: Asset Value Assessment

---

<b>Asset</b>	<b>Value</b>	<b>Numeric Value</b>	<b>Rationale</b>
6. Mechanical Systems			
7. Plumbing and Gas Systems			
8. Electrical Systems			
9. Fire Alarm Systems			
10. IT/Communications Systems			

**This page intentionally left blank**

## Unit III

---

**COURSE TITLE**

Building Design for Homeland Security

---

**UNIT TITLE**

Threat/Hazard Assessment

---

**OBJECTIVES**

1. Identify the threats and hazards that may impact a building or site
  2. Define each threat and hazard using the Department of Defense methodology
  3. Provide a numerical rating for the threat or hazard and justify the basis for the rating
  4. Define the Design Basis Threat and Levels of Protection
- 

**SCOPE**

The following topics will be covered in this unit:

1. From what offices is threat and hazard information available.
  2. The spectrum of event profiles for terrorism and technological hazards from FEMA 386-7.
  3. The five components used by DoD to define a threat and how it can be applied to the Homeland Security Advisory System.
  4. Various approaches to determine threat rating – Federal Emergency Management Agency, Department of Defense, Department of Justice, and Veterans Affairs.
  5. A rating scale and how to use it to determine a threat rating.
  6. Activity: Identify the threats and hazards to consider in the Case Study. As an absolute minimum, consider explosive blast and agents (chemical, biological, and radiological). Determine the threat rating for the minimum threat/hazards.
- 

**REFERENCES**

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, pages 1-1 to 1-18
2. Case Study – Hazardville Information Company

---

**This page intentionally left blank**

### UNIT III CASE STUDY ACTIVITY: THREAT/HAZARD RATINGS

After assets that need to be protected are determined, an assessment is performed to identify the threats and hazards that could cause harm to the building and the inhabitants of the building. Hazards are categorized into two groups: natural and manmade. While natural hazards could logically be expected to affect the HIC, the Case Study only describes the threat from explosive blast and from chemical, biological, and/or radiological “agents.”

The result of this assessment is a “Threat Rating.” The threat rating is a subjective judgment of a threat based on existence, capability, history, intentions, and targeting. The rating scale is a scale of 1 to 10, with 1 a very low probability of a terrorist attack and 10 a very high probability.

#### Requirements

Refer to the HIC Case Study data and GIS portfolio and complete the following worksheets. Each student will interpret the HIC threat information and should have a number close to the value shown. Any function with key IT systems connected to the Internet should get high cyber values. Functions that are susceptible to blast should get high numbers. A CBR attack will impact the entire facility.

#### HIC Critical Functions Threat Rating

Function	Cyber Attack	Armed Attack	Vehicle Bomb	CBR Attack	Rationale
1. Administration	6	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
2. Engineering/IT Technicians	5	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be

Function	Cyber Attack	Armed Attack	Vehicle Bomb	CBR Attack	Rationale
					in the area.
3. Loading Dock/Warehousing					
4. Data Center					
5. Communications					
6. Security					
7. Housekeeping					

**HIC Infrastructure Threat Rating**

Function	Cyber Attack	Armed Attack	Vehicle Bomb	CBR Attack	Rationale
1. Site					

<b>Function</b>	<b>Cyber Attack</b>	<b>Armed Attack</b>	<b>Vehicle Bomb</b>	<b>CBR Attack</b>	<b>Rationale</b>
2. Architectural					
3. Structural					
4. Envelope Systems					
5. Utility Systems					
6. Mechanical Systems					
7. Plumbing and Gas Systems					
8. Electrical Systems					
9. Fire Alarm Systems					

**Course Title: Building Design for Homeland Security**

Unit III: Threat/Hazard Assessment

---

<b>Function</b>	<b>Cyber Attack</b>	<b>Armed Attack</b>	<b>Vehicle Bomb</b>	<b>CBR Attack</b>	<b>Rationale</b>
10. IT/Communications Systems					

**This page intentionally left blank**

## Unit IV

---

**COURSE TITLE**

Building Design for Homeland Security

---

**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 – Federal Emergency Management Agency, Department of Defense, Department of Justice, and Veterans Affairs.
  3. A rating scale and how to use it to determine a vulnerability rating.
  4. Activity: Identify the vulnerabilities present in the Case Study. As an absolute minimum, consider threats/hazards associated with explosive blast and agents (chemical, biological, and radiological). Determine the vulnerability rating for each asset – threat/hazard pairs of interest.
- 

**REFERENCES**

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, Chapter 1
2. Case Study – Hazardville Information Company

---

**This page intentionally left blank**

### UNIT IV CASE STUDY ACTIVITY: VULNERABILITY RATING

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 pair. In-depth vulnerability assessment of a building evaluates specific design and architectural features and identifies all vulnerabilities of the building functions and building systems.

#### Requirement

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 Questions	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: <i>GSA PBS-100</i>	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.

Section	Vulnerability Questions	Guidance	Observations
1.19	Do site landscaping and street furniture provide hiding places?	<p>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.</p> <p>If mail or express boxes are used, the size of the openings should be restricted to prohibit the insertion of packages.</p> <p>Reference: <i>GSA PBS-100</i></p>	
2.15	<p>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?</p> <p>Are the critical building systems and components hardened?</p>	<p>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; and 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 back-up 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.</p> <p>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.</p> <p>Reference: <i>GSA PBS-100</i></p>	

Section	Vulnerability Questions	Guidance	Observations
2.16	<p>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?</p>	<p>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: <i>GSA PBS-100</i></p>	
4.2	<p>Is there less than 40 percent fenestration openings per structural bay?</p> <p>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.)</p>	<p>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.</p> <p>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.</p> <p>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</p>	

**Course Title: Building Design for Homeland Security**

Unit IV: Vulnerability Assessment

<b>Section</b>	<b>Vulnerability Questions</b>	<b>Guidance</b>	<b>Observations</b>
		the angle of incidence of the blast wave upon upper story windows (4th floor and higher). Reference: <i>GSA PBS-100</i>	

## HIC Critical Functions Vulnerability Rating

### Requirement

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

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

### HIC Infrastructure Vulnerability Rating

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

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

## Unit V

---

**COURSE TITLE**

Building Design for Homeland Security

---

**UNIT TITLE**

Risk Assessment/Risk Management

---

**OBJECTIVES**

1. Explain what constitutes risk
  2. Evaluate risk using the Threat-Vulnerability Matrix to capture assessment information
  3. Provide a numerical rating for risk and justify the basis for the rating
  4. Identify top risks for asset – threat/hazard pairs that should receive measures to mitigate vulnerabilities and reduce risk
- 

**SCOPE**

The following topics will be covered in this unit:

1. Definition of risk and the various components to determine a risk rating.
  2. The FEMA 426 approach to determining risk.
  3. A rating scale and how to use it to determine a risk rating. One or more specific examples will be used to focus students on the following activity.
  4. The relationships between high risk, the need for mitigation measures, and the need to identify a Design Basis Threat and Level of Protection.
  5. Activity: Determine the risk rating for the asset – threat/hazard pairs of interest. Identify the top three risk ratings for the Case Study.
- 

**REFERENCES**

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, Chapter 1
2. Case Study – Hazardville Information Company

---

**This page intentionally left blank**

## UNIT V CASE STUDY ACTIVITY: RISK RATING

One approach to conducting a risk assessment is to assemble the results of the asset value assessment, the threat assessment, and the vulnerability assessment, and determine a numeric value of risk for each asset-threat/hazard pair using the following formula:

$$\text{Risk} = \text{Asset Value} \times \text{Threat Rating} \times \text{Vulnerability Rating}$$

### Requirement

Use the following tables to summarize the HIC asset, threat, and vulnerability assessments conducted in the previous three unit activities. Then use the formula above to determine the risk rating for each asset-threat/hazard pair identified under Critical Functions and under Critical Infrastructure. Using **Figure 1-13 of FEMA 426**, make a determination of the available risk management options.

### Critical Functions

Function	Cyber Attack	Armed Attack	Vehicle Bomb	CBR Attack
<b>1. Administration Risk Rating</b>	192	96	192	128
Asset Value	4	4	4	4
Threat Rating	6	3	6	4
Vulnerability Rating	8	8	8	8
<b>2. Engineering/IT Technicians Risk Rating</b>	200	120	240	160
Asset Value	5	5	5	5
Threat Rating	5	3	6	4
Vulnerability Rating	8	8	8	8
<b>3. Loading Dock/ Warehouse Risk Rating</b>				
Asset Value				
Threat Rating				
Vulnerability Rating				

<b>4. Data Center Risk Rating</b>				
Asset Value				
Threat Rating				
Vulnerability Rating				
<b>5. Communications Risk Rating</b>				
Asset Value				
Threat Rating				
Vulnerability Rating				
<b>6. Security Risk Rating</b>				
Asset Value				
Threat Rating				
Vulnerability Rating				
<b>7. Housekeeping Risk Rating</b>				
Asset Value				
Threat Rating				
Vulnerability Rating				

**Critical Infrastructure**

<b>Infrastructure</b>	<b>Cyber Attack</b>	<b>Armed Attack</b>	<b>Vehicle Bomb</b>	<b>CBR Attack</b>
<b>1. Site Risk Rating</b>				
Asset Value				
Threat Rating				
Vulnerability Rating				
<b>2. Architectural Risk Rating</b>				
Asset Value				
Threat Rating				
Vulnerability Rating				
<b>3. Structural Systems Risk Rating</b>				
Asset Value				
Threat Rating				
Vulnerability Rating				

<b>Infrastructure</b>	<b>Cyber Attack</b>	<b>Armed Attack</b>	<b>Vehicle Bomb</b>	<b>CBR Attack</b>
<b>4. Envelope Systems Risk Rating</b>				
Asset Value				
Threat Rating				
Vulnerability Rating				
<b>5. Utility Systems Risk Rating</b>				
Asset Value				
Threat Rating				
Vulnerability Rating				
<b>6. Mechanical Systems Risk Rating</b>				
Asset Value				
Threat Rating				
Vulnerability Rating				
<b>7. Plumbing and Gas Systems Risk Rating</b>				
Asset Value				
Threat Rating				
Vulnerability Rating				
<b>8. Electrical Systems Risk Rating</b>				
Asset Value				
Threat Rating				
Vulnerability Rating				
<b>9. Fire Alarm Systems Risk Rating</b>				
Asset Value				
Threat Rating				
Vulnerability Rating				
<b>10. IT/Communications Systems Risk Rating</b>				
Asset Value				
Threat Rating				
Vulnerability Rating				

**This page intentionally left blank**

## Unit VI

---

**COURSE TITLE**

Building Design for Homeland Security

---

**UNIT TITLE**

Explosive Blast

---

**OBJECTIVES**

1. Explain the basic physics involved during an explosive blast event, whether by terrorism or technological accident
  2. Explain building damage and personnel injury resulting from the blast effects upon a building
  3. Perform an initial prediction of blast loading and effects based upon incident pressure
- 

**SCOPE**

The following topics will be covered in this unit:

1. Time-pressure regions of a blast event and how these change with distance from the blast
  2. Difference between incident pressure and reflected pressure
  3. Differences between peak pressure and peak impulse and how these differences affect building components
  4. Building damage and personal injuries generated by blast wave effects
  5. Levels of protection used by the Department of Defense and the General Services Administration
  6. The nominal range-to-effect chart [minimum stand-off in feet versus weapon yield in pounds of TNT-equivalent] for an identified level of damage or injury
  7. The benefits of stand-off distance
  8. Approaches to predicting blast loads and effects, including one using incident pressure
- 

**REFERENCES**

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*
2. Case Study – Hazardville Information Company

---

**This page intentionally left blank**

**UNIT VI CASE STUDY ACTIVITY:  
EXPLOSIVES ENVIRONMENT AND STAND-OFF DISTANCE AND THE EFFECTS  
OF BLAST**

The requirements in this Unit's activity are intended to provide a check on learning about explosive blast.

**Requirement**

1. In the empty cells in the table below, identify whether the adjacent description defines incident pressure or reflected pressure.

Definition	Type of Pressure
Characterized by an almost instantaneous rise from atmospheric pressure to peak overpressure.	
When it impinges on a structure that is not parallel to the direction of the wave's travel, the pressure wave is reflected and reinforced.	

2. Refer to **Figure 4-5 in FEMA 426 (page 4-11)** to answer the following questions regarding the explosives environment:

- What is the minimum stand-off distance from a 100-pound bomb explosion to eliminate the danger of glass breakage and severe wounds (without fragment retention film)?
- What damage will be sustained at 400 feet from a 5,000-pound bomb explosion?

3. Refer to **Figure 4-10 and Table 4-3 in FEMA 426 (pages 4-17 and 4-19, respectively)** to answer the following questions regarding the explosives environment.

- What is the minimum stand-off required to limit the incident pressure to under 0.5 psi for a 100-pound bomb?
- What incident pressure would be expected at 500 feet from a 500-pound bomb and what is the approximate damage?

**This page intentionally left blank**

## Unit VII

---

**COURSE TITLE**

Building Design for Homeland Security

---

**UNIT TITLE**

Chemical, Biological, and Radiological (CBR) Measures

---

**OBJECTIVES**

1. Explain the five possible protective actions for a building and its occupants
  2. Compare filtration and collection mechanisms and applicability to the particles present in chemical, biological, and radiological agents
  3. Explain the key issues with CBR detection
  4. Identify the indications of CBR contamination
- 

**SCOPE**

This unit will cover the following topics:

1. Five protective actions for a building and its occupants: evacuation; sheltering in place; personal protective equipment; air filtration and pressurization; and exhausting and purging
  2. Air filtration and cleaning principles and its application
  3. CBR detection technology currently available
  4. Indications of CBR contamination that do not use technology
- 

**REFERENCES**

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, pages 5-1 to 5-36
  2. FEMA 426, Appendix C, Chemical, Biological, and Radiological Glossary
  3. Case Study – Hazardville Information Company
-

---

**This page intentionally left blank**

**UNIT VII CASE STUDY ACTIVITY:  
CHEMICAL, BIOLOGICAL AND RADIOLOGICAL (CBR) CONSIDERATIONS**

The requirements in this Unit's activity are intended to provide a check on learning about the nature of chemical, biological, and radiological agents.

**Requirement**

1. Review the HIC case study and name the prevalent CBR threat(s) to the HIC.

Refer to **Table 5-1 on page 5-12 of FEMA 426** and answer the following questions:

2. What size filtration unit (MERV) is required to filter out 75 percent of Legionella and dust particulates (1 to 3 microns) inside the HIC?
3. What range of MERV is required to remove 85 percent of smoke particles greater than 0.3 micron in size?
4. What mitigation measure can be used in the HVAC systems to destroy bacteria and viruses?

---

**This page intentionally left blank**

## Unit VIII

---

**COURSE TITLE**

Building Design for Homeland Security

---

**UNIT TITLE**

Site and Layout Design Guidance

---

**OBJECTIVES**

1. Explain the concerns of land use as applied to threats and hazards due to terrorism and technological accidents
  2. Identify site planning concerns that can create, reduce, or eliminate vulnerabilities and understand the concept of “Layers of Defense”
  3. Compare the pros and cons of barrier mitigation measures that increase stand-off or create controlled access zones
  4. Identify the positive and negative aspects of mitigation approaches for entry control and vehicle access, signage, parking, loading docks, lighting, and site utilities
  5. Explain the basic concepts of Crime Prevention Through Environmental Design (CPTED) and its applicability to building security against terrorism
  6. Apply these concepts to an existing site or building and identify mitigation measures needed to reduce vulnerabilities
- 

**SCOPE**

This unit will cover the following topics:

1. Land use considerations both outside and inside the property line
  2. Site planning issues to include site design, layout and form, vehicular and pedestrian circulation, and landscape and urban design
  3. Creating stand-off distance using perimeter controls, non-exclusive zones, and exclusive zones along with the design concepts and technology to consider
  4. Design considerations and mitigation measures for building security
- 

**REFERENCES**

1. Course Goal and Objectives
2. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings Chapter 2*
3. Unit VIII Visuals

**This page intentionally left blank**

### UNIT VIII CASE STUDY ACTIVITY: SITE AND LAYOUT DESIGN GUIDANCE

The Building Vulnerability Assessment Checklist in FEMA 426 can be used as a screening tool for preliminary design vulnerability assessment. The checklist includes questions that determine if critical systems will continue to function to enhance deterrence, detection, denial, and damage limitation, and emergency systems function during a threat or hazard situation.

#### Requirement

Assign sections of the checklist to the group member who is most knowledgeable and qualified to perform an assessment of the assigned area. Refer to the HIC case study and to the GIS portfolio to determine answers to the questions. Then review results to identify vulnerabilities and possible mitigation measures.

1. Complete the following components of the Building Vulnerability Assessment Checklist which address site and layout.
2. Upon completion of these portions of the checklist, refer back to the site risk rating determined in Unit V Case Study Activity and, based on this detailed analysis, decide if the rating is accurate.
3. Select mitigation measures to reduce vulnerability and associated risk from the site and layout perspective.
4. Estimate the new risk ratings for high risk asset-threat pairs based on the recommended mitigation measures.

Section	Vulnerability Questions	Guidance	Observations
1.1	<p>What major structures surround the facility (site or building(s))?</p> <p>What critical infrastructure, government, military, or recreation facilities are in the local area that impact transportation, utilities, and collateral damage (attack at this facility impacting the other major structures or attack on the major structures impacting this facility)?</p>	<p><b>Critical infrastructure to consider includes:</b> <b>Telecommunications infrastructure</b> Facilities for broadcast TV, cable TV; cellular networks; newspaper offices, production, and distribution; radio stations; satellite base stations; telephone trunking and switching stations, including critical cable routes and major rights-of-way <b>Electric power systems</b> Power plants, especially nuclear facilities; transmission and distribution system components; fuel distribution, delivery, and storage</p>	

Section	Vulnerability Questions	Guidance	Observations
		<p><b>Gas and oil facilities</b>                      Hazardous material facilities, oil/gas pipelines, and storage facilities</p> <p><b>Banking and finance institutions</b>                      Financial institutions (banks, credit unions) and the business district; note schedule business/financial district may follow; armored car services</p> <p><b>Transportation networks</b>                      Airports: carriers, flight paths, and airport layout; location of air traffic control towers, runways, passenger terminals, and parking areas                      Bus Stations:                      Pipelines: oil; gas                      Trains/Subways: rails and lines, railheads/rail yards, interchanges, tunnels, and cargo/passenger terminals; note hazardous material transported                      Traffic: interstate highways/roads/tunnels/ bridges carrying large volumes; points of congestion; note time of day and day of week                      Trucking: hazardous materials cargo loading/unloading facilities; truck terminals, weigh stations, and rest areas                      Waterways: dams; levees; berths and ports for cruise ships, ferries, roll-on/roll-off cargo vessels, and container ships; international (foreign) flagged vessels (and cargo)</p> <p><b>Water supply systems</b>                      Pipelines and process/treatment facilities, dams for water collection; wastewater treatment</p> <p><b>Government services</b>                      Federal/state/local government offices – post offices, law enforcement stations, fire/rescue, town/city hall, local mayor’s/governor’s residences, judicial offices and courts, military installations (include type-active, Reserves, National Guard)</p>	

Section	Vulnerability Questions	Guidance	Observations
		<p><b>Emergency services</b>                      Backup facilities,                      communications centers,                      Emergency Operations Centers (EOCs), fire/Emergency Medical Service (EMS) facilities,                      Emergency Medical Centers (EMCs), law enforcement facilities</p> <p><b>The following are not critical infrastructure, but have collateral damage potential to consider:</b></p> <p><b>Agricultural facilities:</b>                      chemical distribution, storage, and application sites; crop spraying services; farms and ranches; food processing, storage, and distribution facilities</p> <p><b>Commercial/manufacturing/industrial facilities:</b> apartment buildings; business/corporate centers; chemical plants (especially those with Section 302 Extremely Hazardous Substances); factories; fuel production, distribution, and storage facilities; hotels and convention centers; industrial plants; raw material production, distribution, and storage facilities; research facilities and laboratories; shipping, warehousing, transfer, and logistical centers</p> <p><b>Events and attractions:</b>                      festivals and celebrations; open-air markets; parades; rallies, demonstrations, and marches; religious services; scenic tours; theme parks</p> <p><b>Health care system components:</b> family planning clinics; health department offices; hospitals; radiological material and medical waste transportation, storage, and disposal; research facilities and laboratories, walk-in clinics</p> <p><b>Political or symbolically significant sites:</b> embassies, consulates, landmarks, monuments, political party and</p>	

Section	Vulnerability Questions	Guidance	Observations
		<p>special interest groups offices, religious sites</p> <p><b>Public/private institutions:</b> academic institutions, cultural centers, libraries, museums, research facilities and laboratories, schools</p> <p><b>Recreation facilities:</b> auditoriums, casinos, concert halls and pavilions, parks, restaurants and clubs (frequented by potential target populations), sports arenas, stadiums, theaters, malls, and special interest group facilities; note congestion date and times for shopping centers</p> <p>References: <i>FEMA 386-7, FEMA SLG 101, DOJ NCJ181200</i></p>	
1.2	Does the terrain place the building in a depression or low area?	<p>Depressions or low areas can trap heavy vapors, inhibit natural decontamination by prevailing winds, and reduce the effectiveness of in-place sheltering.</p> <p>Reference: <i>USAF Installation Force Protection Guide</i></p>	
1.3	In dense, urban areas, does curb lane parking place uncontrolled parked vehicles unacceptably close to a building in public rights-of-way?	<p>Where distance from the building to the nearest curb provides insufficient setback, restrict parking in the curb lane. For typical city streets, this may require negotiating to close the curb lane. Setback is common terminology for the distance between a building and its associated roadway or parking. It is analogous to stand-off between a vehicle bomb and the building. The benefit per foot of increased stand-off between a potential vehicle bomb and a building is very high when close to a building and decreases rapidly as the distance increases. Note that the July 1, 1994, Americans with Disabilities Act Standards for Accessible Design states that required handicapped parking shall be located on the shortest accessible route of travel from adjacent parking to an accessible entrance.</p>	

Section	Vulnerability Questions	Guidance	Observations
		Reference: <i>GSA PBS-P100</i>	
1.4	Is a perimeter fence or other types of barrier controls in place?	The intent is to channel pedestrian traffic onto a site with multiple buildings through known access control points. For a single building, the intent is to have a single visitor entrance. Reference: <i>GSA PBS-P100</i>	
1.5	What are the site access points to the site or building?	The goal is to have at least two access points – one for passenger vehicles and one for delivery trucks due to the different procedures needed for each. Having two access points also helps if one of the access points becomes unusable, then traffic can be routed through the other access point. Reference: <i>USAF Installation Force Protection Guide</i>	
1.6	Is vehicle traffic separated from pedestrian traffic on the site?	Pedestrian access should not be endangered by car traffic. Pedestrian access, especially from public transportation, should not cross vehicle traffic if possible. Reference: <i>GSA PBS-P100 and FEMA 386-7</i>	
1.7	Is there vehicle and pedestrian access control at the perimeter of the site?	Vehicle and pedestrian access control and inspection should occur as far from facilities as possible (preferably at the site perimeter) with the ability to regulate the flow of people and vehicles one at a time.  Control on-site parking with identification checks, security personnel, and access control systems. Reference: <i>FEMA 386-7</i>	
1.8	Is there space for inspection at the curb line or outside the protected perimeter?  What is the minimum distance from the inspection location to the building?	Design features for the vehicular inspection point include: vehicle arrest devices that prevent vehicles from leaving the vehicular inspection area and prevent tailgating.  If screening space cannot be provided, consider other design features such as: hardening and alternative location for vehicle search/ inspection. Reference: <i>GSA PBS-P100</i>	

Section	Vulnerability Questions	Guidance	Observations
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, stormwater runoff culverts, etc. Ensure covers to these access points are secured. Reference: <i>USAF Installation Force Protection Guide</i>	Unknown without a more detailed on-site assessment.
1.10	What are the existing types of vehicle anti-ram devices for the site or building?  Are these devices at the property boundary or at the building?	Passive barriers include bollards, walls, hardened fences (steel cable interlaced), trenches, ponds/basins, concrete planters, street furniture, plantings, trees, sculptures, and fountains. Active barriers include pop-up bollards, swing arm gates, and rotating plates and drums, etc. Reference: <i>GSA PBS-P100</i>	
1.11	What is the anti-ram buffer zone stand-off distance from the building to unscreened vehicles or parking?	If the recommended distance for the postulated threat is not available, consider reducing the stand-off required through structural hardening or manufacturing additional stand-off through barriers and parking restrictions. Also consider relocation of vulnerable functions within the building or to a more hazard-resistant building. More stand-off should be used for unscreened vehicles than for screened vehicles that are searched. Reference: <i>GSA PBS P-100</i>	
1.12	Are perimeter barriers capable of stopping vehicles?  Will the vehicle barriers at the perimeter and building maintain access for emergency responders, including large fire apparatus?	Anti-ram protection may be provided by adequately designed: bollards, street furniture, sculpture, landscaping, walls, and fences. The anti-ram protection must be able to stop the threat vehicle size (weight) at the speed attainable by that vehicle at impact. If the anti-ram protection cannot absorb the desired kinetic energy, consider adding speed controls (serpentines or speed bumps) to limit the speed at impact. If the resultant speed is still too great, the anti-ram protection should be improved. Reference: <i>Military Handbook 1013/14 and GSA PBS P-100</i>	
1.13	Does site circulation	The intent is to use site circulation to minimize vehicle	

Section	Vulnerability Questions	Guidance	Observations
	prevent high-speed approaches by vehicles?	speeds and eliminate direct approaches to structures. Reference: <i>GSA PBS-P100</i>	
1.14	Are there offsetting vehicle entrances from the direction of a vehicle's approach to force a reduction of speed?	Single or double 90-degree turns effectively reduce vehicle approach speed. Reference: <i>GSA PBS-P100</i>	
1.15	Is there a minimum setback distance between the building and parked vehicles?	Adjacent public parking should be directed to more distant or better-protected areas, segregated from employee parking and away from the building. Some publications use the term setback in lieu of the term stand-off. Reference: <i>GSA PBS-P100</i>	
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: <i>GSA PBS-P100</i>	
1.17	Do stand-alone, above ground parking garages provide adequate visibility across as well as into and out of the parking garage?	<p>Pedestrian paths should be planned to concentrate activity to the extent possible.</p> <p>Limiting vehicular entry/exits to a minimum number of locations is beneficial.</p> <p>Stair tower and elevator lobby design shall be as open as code permits. Stair and/or elevator waiting areas should be as open to the exterior and/or the parking areas as possible and well lighted. Impact-resistant, laminated glass for stair towers and elevators is a way to provide visual openness.</p> <p>Potential hiding places below stairs should be closed off; nooks and crannies should be avoided, and dead-end parking areas should be eliminated. Reference: <i>GSA PBS-P100</i></p>	
1.18	Are garage or service area	Control internal building parking, underground parking	

Section	Vulnerability Questions	Guidance	Observations
	<p>entrances for employee-permitted vehicles protected by suitable anti-ram devices?</p> <p>Coordinate this protection with other anti-ram devices, such as on the perimeter or property boundary to avoid duplication of arresting capability.</p>	<p>garages, and access to service areas and loading docks in this manner with proper access control or eliminate the parking altogether.</p> <p>The anti-ram device must be capable of arresting a vehicle of the designated threat size at the speed attainable at the location. Reference: <i>GSA PBS-P100</i></p>	
1.19	<p>Do site landscaping and street furniture provide hiding places?</p>	<p>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.</p> <p>If mail or express boxes are used, the size of the openings should be restricted to prohibit the insertion of packages. Reference: <i>GSA PBS-P100</i></p>	
1.20	<p>Is the site lighting adequate from a security perspective in roadway access and parking areas?</p>	<p>Security protection can be successfully addressed through adequate lighting. The type and design of lighting, including illumination levels, is critical. Illuminating Engineering Society of North America (IESNA) guidelines can be used. The site lighting should be coordinated with the CCTV system. Reference: <i>GSA PBS-P100</i></p>	
1.21	<p>Are line-of-sight perspectives from outside the secured boundary to the building and on the property along pedestrian and vehicle routes integrated with landscaping and green space?</p>	<p>The goal is to prevent the observation of critical assets by persons outside the secure boundary of the site. For individual buildings in an urban environment, this could mean appropriate window treatments or no windows for portions of the building.</p>	

Section	Vulnerability Questions	Guidance	Observations
		Once on the site, the concern is to ensure observation by a general workforce aware of any pedestrians and vehicles outside normal circulation routes or attempting to approach the building unobserved. Reference: <i>USAF Installation Force Protection Guide</i>	
1.22	Do signs provide control of vehicles and people?	The signage should be simple and have the necessary level of clarity. However, signs that identify sensitive areas should generally not be provided. Reference: <i>GSA PBS-P100</i>	
1.23	Are all existing fire hydrants on the site accessible?	Just as vehicle access points to the site must be able to transit emergency vehicles, so too must the emergency vehicles have access to the buildings and, in the case of fire trucks, the fire hydrants. Thus, security considerations must accommodate emergency response requirements. Reference: <i>GSA PBS-P100</i>	
2	Architectural		
2.1	Does the site and architectural design incorporate strategies from a Crime Prevention Through Environmental Design (CPTED) perspective?	<p><b>The focus of CPTED is on creating defensible space by employing:</b></p> <p><b>1. Natural access controls:</b> Design streets, sidewalks, and building entrances to clearly indicate public routes and direct people away from private/restricted areas Discourage access to private areas with structural elements and limit access (no cut-through streets) Loading zones should be separate from public parking</p> <p><b>2. Natural surveillance:</b> Design that maximizes visibility of people, parking areas, and building entrances: doors and windows that look out on to streets and parking areas Shrubbery under 2 feet in height for visibility Lower branches of existing trees kept at least 10 feet off ground Pedestrian-friendly sidewalks</p>	

Section	Vulnerability Questions	Guidance	Observations
		<p>and streets to control pedestrian and vehicle circulation                      Adequate nighttime lighting, especially at exterior doorways  <b>3. Territorial reinforcement:</b>                      Design that defines property lines                      Design that distinguishes private/restricted spaces from public spaces using separation, landscape plantings; pavement designs (pathway and roadway placement); gateway treatments at lobbies, corridors, and door placement; walls, barriers, signage, lighting, and "CPTED" fences                      "Traffic-calming" devices for vehicle speed control  <b>4. Target hardening:</b>                      Prohibit entry or access: window locks, deadbolts for doors, interior door hinges                      Access control (building and employee/visitor parking) and intrusion detection systems  <b>5. Closed circuit television cameras:</b>                      Prevent crime and influence positive behavior, while enhancing the intended uses of space. In other words, design that eliminates or reduces criminal behavior and at the same time encourages people to "keep an eye out" for each other.                      Reference: <i>GSA PBS-P100 and FEMA 386-7</i></p>	
2.2	Is it a mixed-tenant building?	<p>Separate high-risk tenants from low-risk tenants and from publicly accessible areas. Mixed uses may be accommodated through such means as separating entryways, controlling access, and hardening shared partitions, as well as through special security operational countermeasures.                      Reference: <i>GSA PBS-P100</i></p>	
2.3	Are pedestrian paths planned to concentrate activity to aid in detection?	<p>Site planning and landscape design can provide natural surveillance by concentrating pedestrian activity, limiting entrances/exits, and eliminating concealment opportunities. Also, prevent pedestrian access to</p>	

Section	Vulnerability Questions	Guidance	Observations
		parking areas other than via established entrances. Reference: <i>GSA PBS-P100</i> .	
2.4	Are there trash receptacles and mailboxes in close proximity to the building that can be used to hide explosive devices?	The size of the trash receptacles and mailbox openings should be restricted to prohibit insertion of packages. Street furniture, such as newspaper vending machines, should be kept sufficient distance (10 meters or 33 feet) from the building, or brought inside to a secure area. References: <i>USAF Installation Force Protection Guide, DoD Minimum Antiterrorism Standards for Buildings</i>	
5	Utility Systems		
5.1	What is the source of domestic water? (utility, municipal, wells, lake, river, storage tank)  Is there a secure alternate drinking water supply?	Domestic water is critical for continued building operation. Although bottled water can satisfy requirements for drinking water and minimal sanitation, domestic water meets many other needs – flushing toilets, building heating and cooling system operation, cooling of emergency generators, humidification, etc. Reference: <i>FEMA 386-7</i>	Unknown without a more detailed on-site assessment.
5.2	Are there multiple entry points for the water supply?	If the building or site has only one source of water entering at one location, the entry point should be secure. Reference: <i>GSA PBS-P100</i>	Unknown without a more detailed on-site assessment.
5.3	Is the incoming water supply in a secure location?	Ensure that only authorized personnel have access to the water supply and its components. Reference: <i>FEMA 386-7</i>	Unknown without a more detailed on-site assessment.
5.4	Does the building or site have storage capacity for domestic water?  How many gallons and how long will it allow operations to continue?	Operational facilities will require reliance on adequate domestic water supply. Storage capacity can meet short-term needs and use water trucks to replenish for extended outages. Reference: <i>Physical Security Assessment for Department of Veterans Affairs Facilities</i> .	Unknown without a more detailed assessment.
5.5	What is the source of water for the fire suppression system? (local utility company lines, storage tanks with	The fire suppression system water may be supplied from the domestic water or it may have a separate source, separate storage, or nonpotable alternate sources.	Unknown without a more detailed on-site assessment.

Section	Vulnerability Questions	Guidance	Observations
	<p>utility company backup, lake, or river)</p> <p>Are there alternate water supplies for fire suppression?</p>	<p>For a site with multiple buildings, the concern is that the supply should be adequate to fight the worst case situation according to the fire codes. Recent major construction may change that requirement. Reference: <i>FEMA 386-7</i></p>	
5.6	<p>Is the fire suppression system adequate, code-compliant, and protected (secure location)?</p>	<p>Standpipes, water supply control valves, and other system components should be secure or supervised. Reference: <i>FEMA 386-7</i></p>	
5.7	<p>Do the sprinkler/standpipe interior controls (risers) have fire- and blast-resistant separation?</p> <p>Are the sprinkler and standpipe connections adequate and redundant?</p> <p>Are there fire hydrant and water supply connections near the sprinkler/standpipe connections?</p>	<p>The incoming fire protection water line should be encased, buried, or located 50 feet from high risk areas. The interior mains should be looped and sectionalized. Reference: <i>GSA PBS-P100</i></p>	<p>Unknown without a more detailed on-site assessment.</p>
5.8	<p>Are there redundant fire water pumps (e.g., one electric, one diesel)?</p> <p>Are the pumps located apart from each other?</p>	<p>Collocating fire water pumps puts them at risk for a single incident to disable the fire suppression system. Reference: <i>GSA PBS-P100 and FEMA 386-7</i></p>	<p>Unknown without a more detailed on-site assessment.</p>
5.9	<p>Are sewer systems accessible?</p> <p>Are they protected or secured?</p>	<p>Sanitary and stormwater sewers should be protected from unauthorized access. The main concerns are backup or flooding into the building, causing a health risk, shorting out electrical equipment, and loss of building use. Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	<p>Unknown without a more detailed on-site assessment.</p>
5.10	<p>What fuel supplies do the building rely upon for critical operation?</p>	<p>Typically, natural gas, propane, or fuel oil are required for continued operation.</p>	

Section	Vulnerability Questions	Guidance	Observations
		Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
5.11	How much fuel is stored on the site or at the building and how long can this quantity support critical operations?  How is it stored?  How is it secured?	Fuel storage protection is essential for continued operation.  Main fuel storage should be located away from loading docks, entrances, and parking. Access should be restricted and protected (e.g., locks on caps and seals). References: <i>GSA PBS-P100 and Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
5.12	Where is the fuel supply obtained?  How is it delivered?	The supply of fuel is dependent on the reliability of the supplier. Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
5.13	Are there alternate sources of fuel?  Can alternate fuels be used?	Critical functions may be served by alternate methods if normal fuel supply is interrupted. Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
5.14	What is the normal source of electrical service for the site or building?	Utilities are the general source unless co-generation or a private energy provider is available. Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
5.15	Is there a redundant electrical service source?  Can the site or buildings be fed from more than one utility substation?	The utility may have only one source of power from a single substation. There may be only single feeders from the main substation. Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	Unknown without a more detailed on-site assessment.
5.16	How many service entry points does the site or building have for electricity?	Electrical supply at one location creates a vulnerable situation unless an alternate source is available.  Ensure disconnecting requirements according to NFPA 70 (National Fire Protection Association, National Electric Code) are met for multiple service entrances. Reference: <i>Physical Security</i>	Unknown without a more detailed on-site assessment.

Section	Vulnerability Questions	Guidance	Observations
		<i>Assessment for the Department of Veterans Affairs Facilities</i>	
5.17	Is the incoming electric service to the building secure?	Typically, the service entrance is a locked room, inaccessible to the public. Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	Unknown without a more detailed on-site assessment.
5.18	What provisions for emergency power exist? What systems receive emergency power and have capacity requirements been tested?  Is the emergency power co-located with the commercial electric service?  Is there an exterior connection for emergency power?	Besides installed generators to supply emergency power, portable generators or rental generators available under emergency contract can be quickly connected to a building with an exterior quick disconnect already installed.  Testing under actual loading and operational conditions ensures the critical systems requiring emergency power receive it with a high assurance of reliability. Reference: <i>GSA PBS-P100</i>	
5.19	By what means does the main telephone and data communications interface the site or building?	Typically communication ducts or other conduits are available. Overhead service is more identifiable and vulnerable Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
5.20	Are there multiple or redundant locations for the telephone and communication service?	Secure locations of communications wiring entry to the site or building are required. Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	Unknown without a more detailed on-site assessment.
5.21	Does the fire alarm system require communication with external sources?  By what method is the alarm signal sent to the	Typically, the local fire department responds to an alarm that sounds at the station or is transmitted over phone lines by an auto dialer.  An intermediary control center	

**Course Title: Building Design for Homeland Security**

Unit VIII: Site and Layout Design Guidance

---

<b>Section</b>	<b>Vulnerability Questions</b>	<b>Guidance</b>	<b>Observations</b>
	responding agency: telephone, radio, etc?  Is there an intermediary alarm monitoring center?	for fire, security, and/or building system alarms may receive the initial notification at an on-site or off-site location. This center may then determine the necessary response and inform the responding agency.  Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
5.22	Are utility lifelines aboveground, underground, or direct buried?	Utility lifelines (water, power, communications, etc.) can be protected by concealing, burying, or encasing. Reference: <i>GSA PBS-P100 and FEMA 386-7</i>	

## Unit IX

---

**COURSE TITLE**

Building Design for Homeland Security

---

**UNIT TITLE**

Building Design Guidance

---

**OBJECTIVES**

1. Explain architectural considerations to mitigate impacts from blast effects and transmission of chemical, biological, and radiological agents from exterior and interior incidents
  2. Identify key elements of building structural and non-structural systems for mitigation of blast effects
  3. Compare and contrast the benefit of building envelope, mechanical system, electrical system, fire protection system, and communication system mitigation measures, including synergies and conflicts
  4. Apply these concepts to an existing building or building conceptual design and identify mitigation measures needed to reduce vulnerabilities
- 

**SCOPE**

The following topics will be covered in this unit:

1. Architectural considerations, including building configuration, space design, and special situations
  2. Building structural and nonstructural considerations with emphasis on progressive collapse, loads and stresses, and good engineering practices
  3. Design issues for the building envelope, including wall design, window design, door design, and roof system design with approaches to define levels of protection
  4. Mechanical system design issues, including interfacing with operational procedures, emergency plans, and training
  5. Other building systems design consideration for electrical, fire protection, communications, electronic security, entry control, and physical security that mitigate the effects of a threat or hazard
  6. Do an Activity that encompasses identified high risk pairs (asset – threat/hazard) in the threat-vulnerability matrix developed for the Case Study and select mitigation measures that reduce vulnerability and associated risk from the building perspective
-

---

## REFERENCES

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, pages 3-1 to 3-46 and 3-48 to 3-52; Checklist at end of Chapter 1
2. FEMA 427, *Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks*
3. FEMA 430, *Primer for Incorporating Building Security Components in Architectural Design*
4. Case Study – Hazardville Information Company

### UNIT IX CASE STUDY ACTIVITY: BUILDING DESIGN GUIDANCE

In this Unit, the emphasis will be upon providing a balanced building envelope that is a defensive layer against the terrorist tactic of interest and avoiding situations where one incident affects more than one building system. The **Building Vulnerability Assessment Checklist in FEMA 426** can be used as a screening tool for preliminary building design vulnerability assessment.

#### Requirement

Assign sections of the checklist to the group member who is most knowledgeable and qualified to perform an assessment of the assigned area. Refer to the HIC Case Study and to the vulnerability portfolio to determine answers to the questions. Then review results to identify vulnerabilities and possible mitigation measures.

1. Complete the following components of the Building Vulnerability Assessment Checklist that address building design.
2. Upon completion of these portions of the checklist, refer back to the risk ratings determined in Unit V Case Study Activity and, based on this more detailed analysis, decide if the rating is accurate.
3. Select mitigation measures to reduce vulnerability and associated risk from building design.
4. Estimate the new risk ratings for high risk asset-threat pairs based on the recommended mitigation measures.

Section	Vulnerability Questions	Guidance	Observations
2.5	Do entrances avoid significant queuing?	If queuing will occur within the building footprint, the area should be enclosed in blast-resistant construction. If queuing is expected outside the building, a rain cover should be provided. For manpower and equipment requirements, collocate or combine staff and visitor entrances. Reference: <i>GSA PBS-P100</i>	
2.6	Does security screening cover all public and private areas?  Are public and private	Retail activities should be prohibited in non-secured areas. However, the Public Building Cooperative Use Act of 1976 encourages retail and mixed uses to create open and inviting	Unknown without a more detailed on-site assessment.

Section	Vulnerability Questions	Guidance	Observations
	<p>activities separated?</p> <p>Are public toilets, service spaces, or access to stairs or elevators located in any non-secure areas, including the queuing area before screening at the public entrance?</p>	<p>buildings. Consider separating entryways, controlling access, hardening shared partitions, and special security operational countermeasures. References: <i>GSA PBS-P100 and FEMA 386-7</i></p>	
2.7	<p>Is access control provided through main entrance points for employees and visitors? (lobby receptionist, sign-in, staff escorts, issue of visitor badges, checking forms of personal identification, electronic access control systems)</p>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
2.8	<p>Is access to private and public space or restricted area space clearly defined through the design of the space, signage, use of electronic security devices, etc.?</p>	<p>Finishes and signage should be designed for visual simplicity. Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
2.9	<p>Is access to elevators distinguished as to those that are designated only for employees and visitors?</p>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
2.10	<p>Do public and employee entrances include space for possible future installation of access</p>	<p>These include walk-through metal detectors and x-ray devices, identification check, electronic access card, search stations, and turnstiles.</p>	

Section	Vulnerability Questions	Guidance	Observations
	control and screening equipment?	Reference: <i>GSA PBS-P100</i>	
2.11	Do foyers have reinforced concrete walls and offset interior and exterior doors from each other?	Consider for exterior entrances to the building or to access critical areas within the building if explosive blast hazard must be mitigated. Reference: <i>U.S. Army TM 5-853</i>	
2.12	Do doors and walls along the line of security screening meet requirements of UL752 "Standard for Safety: Bullet-Resisting Equipment"?	If the postulated threat in designing entrance access control includes rifles, pistols, or shotguns, then the screening area should have bullet-resistance to protect security personnel and uninvolved bystanders. Glass, if present, should also be bullet-resistant. Reference: <i>GSA PBS-P100</i>	Unknown without a more detailed on-site assessment.
2.13	Do circulation routes have unobstructed views of people approaching controlled access points?	This applies to building entrances and to critical areas within the building. References: <i>USAF Installation Force Protection Guide and DoD UFC 4-010-01</i>	
2.14	Is roof access limited to authorized personnel by means of locking mechanisms?	References: <i>GSA PBS-P100 and CDC/NIOSH, Pub 2002-139</i>	Unknown without a more detailed on-site assessment.
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	

Section	Vulnerability Questions	Guidance	Observations
		<p>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.</p> <p>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: <i>GSA PBS-P100</i></p>	
2.16	<p>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?</p>	<p>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: <i>GSA PBS-P100</i></p>	
2.17	<p>Is high visitor activity away from critical assets?</p>	<p>High-risk activities should also be separated from low-risk activities. Also, visitor activities should be separated from daily activities. Reference: <i>USAF Installation Force Protection Guide</i></p>	
2.18	<p>Are critical assets located in spaces that are occupied 24 hours per day?</p> <p>Are assets located in areas where they are visible to more than one person?</p>	<p>Reference: <i>USAF Installation Force Protection Guide</i></p>	<p>Unknown without a more detailed on-site assessment.</p>
2.19	<p>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</p>	<p>Loading docks should be designed to keep vehicles from driving into or parking under the building. If loading docks are in close proximity to critical equipment, consider hardening the equipment and service against explosive blast. Consider a 50-foot separation distance in all directions. Reference: <i>GSA PBS-P100</i></p>	

Section	Vulnerability Questions	Guidance	Observations
	mains, cooling and heating mains, etc.?		
2.20	<p>Are mailrooms located away from building main entrances, areas containing critical services, utilities, distribution systems, and important assets?</p> <p>Is the mailroom located near the loading dock?</p>	<p>The mailroom should be located at the perimeter of the building with an outside wall or window designed for pressure relief.</p> <p>By separating the mailroom and the loading dock, the collateral damage of an incident at one has less impact upon the other. However, this may be the preferred mailroom location.</p> <p>Off-site screening stations or a separate delivery processing building on site may be cost-effective, particularly if several buildings may share one mailroom. A separate delivery processing building reduces risk and simplifies protection measures.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
2.21	Does the mailroom have adequate space available for equipment to examine incoming packages and for an explosive disposal container?	<p>Screening of all deliveries to the building, including U.S. mail, commercial package delivery services, delivery of office supplies, etc.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
2.22	Are areas of refuge identified, with special consideration given to egress?	<p>Areas of refuge can be safe havens, shelters, or protected spaces for use during specified hazards.</p> <p>Reference: <i>FEMA 386-7</i></p>	
2.23	<p>Are stairwells required for emergency egress located as remotely as possible from high-risk areas where blast events might occur?</p> <p>Are stairways maintained with positive pressure or are there other smoke control systems?</p>	<p>Consider designing stairs so that they discharge into other than lobbies, parking, or loading areas.</p> <p>Maintaining positive pressure from a clean source of air (may require special filtering) aids in egress by keeping smoke, heat, toxic fumes, etc. out of the stairway. Pressurize exit stairways in accordance with the National Model Building Code.</p> <p>References: <i>GSA PBS-P100 and CDC/NIOSH, Pub 2002-139</i></p>	<p>Unknown without a more detailed on-site assessment</p>

Section	Vulnerability Questions	Guidance	Observations
2.24	Are enclosures for emergency egress hardened to limit the extent of debris that might otherwise impede safe passage and reduce the flow of evacuees?	Egress pathways should be hardened and discharge into safe areas. Reference: <i>FEMA 386-7</i>	Unknown without a more detailed on-site assessment.
2.25	Do interior barriers differentiate level of security within a building?	Reference: <i>USAF Installation Force Protection Guide</i>	
2.26	Are emergency systems located away from high-risk areas?	The intent is to keep the emergency systems out of harm's way, such that one incident takes out all capability – both the regular systems and their backups. Reference: <i>FEMA 386-7</i>	
2.27	Is interior glazing near high-threat areas minimized?  Is interior glazing in other areas shatter resistant?	Interior glazing should be minimized where a threat exists and should be avoided in enclosures of critical functions next to high-risk areas. Reference: <i>GSA PBS-P100</i>	Unknown without more detailed on-site assessment.
2.28	Are ceiling and lighting systems designed to remain in place during hazard events?	When an explosive blast shatters a window, the blast wave enters the interior space, putting structural and nonstructural building components under loads not considered in standard building codes. It has been shown that connection criteria for these systems in high seismic activity areas resulted in much less falling debris that could injure building occupants.  Mount all overhead utilities and other fixtures weighing 14 kilograms (31 pounds) or more to minimize the likelihood that they will fall and injure building occupants. Design all equipment mountings to resist forces of 0.5 times the equipment weight in any direction and 1.5 times the equipment weight in the downward direction. This	Unknown without a more detailed on-site assessment.

Section	Vulnerability Questions	Guidance	Observations
		standard does not preclude the need to design equipment mountings for forces required by other criteria, such as seismic standards. Reference: <i>DoD Minimum Antiterrorism Standards for Buildings</i>	
<b>3</b>	<b>Structural Systems</b>		
3.1	What type of construction?  What type of concrete & reinforcing steel?  What type of steel?  What type of foundation?	The type of construction provides an indication of the robustness to abnormal loading and load reversals. A reinforced concrete moment-resisting frame provides greater ductility and redundancy than a flat-slab or flat-plate construction. The ductility of steel frame with metal deck depends on the connection details and pre-tensioned or post-tensioned construction provides little capacity for abnormal loading patterns and load reversals. The resistance of load-bearing wall structures varies to a great extent, depending on whether the walls are reinforced or un-reinforced. A rapid screening process developed by FEMA for assessing structural hazards identifies the following types of construction with a structural score ranging from 1.0 to 8.5. A higher score indicates a greater capacity to sustain load reversals. Wood buildings of all types - 4.5 to 8.5 Steel moment-resisting frames - 3.5 to 4.5 Braced steel frames - 2.5 to 3.0 Light metal buildings - 5.5 to 6.5 Steel frames with cast-in-place concrete shear walls - 3.5 to 4.5 Steel frames with unreinforced masonry infill walls - 1.5 to 3.0 Concrete moment-resisting frames - 2.0 to 4.0 Concrete shear wall buildings - 3.0 to 4.0	

Section	Vulnerability Questions	Guidance	Observations
		Concrete frames with unreinforced masonry infill walls - 1.5 to 3.0 Tilt-up buildings - 2.0 to 3.5 Precast concrete frame buildings - 1.5 to 2.5 Reinforced masonry - 3.0 to 4.0 Unreinforced masonry - 1.0 to 2.5 References: <i>FEMA 154 and Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
3.2	Do the reinforced concrete structures contain symmetric steel reinforcement (positive and negative faces) in all floor slabs, roof slabs, walls, beams and girders that may be subjected to rebound, uplift and suction pressures? Do the lap splices fully develop the capacity of the reinforcement? Are lap splices and other discontinuities staggered? Do the connections possess ductile details? Is special shear reinforcement, including ties and stirrups, available to allow large post-elastic behavior?	Reference: <i>GSA PBS-P100</i>	Unknown without a more detailed on-site assessment.
3.3	Are the steel frame connections moment connections?  Is the column spacing minimized so that reasonably sized members will resist the design loads and increase the redundancy of the system?	A practical upper level for column spacing is generally 30 feet. Unless there is an overriding architectural requirement, a practical limit for floor-to-floor heights is generally less than or equal to 16 feet. Reference: <i>GSA PBS-P100</i>	Unknown without a more detailed on-site assessment.

Section	Vulnerability Questions	Guidance	Observations
	What are the floor-to-floor heights?		
3.4	Are critical elements vulnerable to failure?	<p>The priority for upgrades should be based on the relative importance of structural or non-structural elements that are essential to mitigating the extent of collapse and minimizing injury and damage.</p> <p>Primary Structural Elements provide the essential parts of the building’s resistance to catastrophic blast loads and progressive collapse. These include columns, girders, roof beams, and the main lateral resistance system.</p> <p>Secondary Structural Elements consist of all other load bearing members, such as floor beams, slabs, etc.</p> <p>Primary Nonstructural Elements consist of elements (including their attachments) which are essential for life safety systems or elements which can cause substantial injury if failure occurs, including ceilings or heavy suspended mechanical units.</p> <p>Secondary Nonstructural Elements consist of all elements not covered in primary nonstructural elements, such as partitions, furniture, and light fixtures.</p> <p>Reference: <i>GSA PBS-P100</i></p>	Unknown without a more detailed on-site assessment.
3.5	Will the structure suffer an unacceptable level of damage resulting from the postulated threat (blast loading or weapon impact)?	<p>The extent of damage to the structure and exterior wall systems from the bomb threat may be related to a protection level. The following is for new buildings:</p> <p>Level of Protection Below Antiterrorism Standards – Severe damage.</p>	

Section	Vulnerability Questions	Guidance	Observations
		<p>Frame collapse/massive destruction. Little left standing. Doors and windows fail and result in lethal hazards. Majority of personnel suffer fatalities.</p> <p>Very Low Level Protection – Heavy damage. Onset of structural collapse. Major deformation of primary and secondary structural members, but progressive collapse is unlikely. Collapse of non-structural elements. Glazing will break and is likely to be propelled into the building, resulting in serious glazing fragment injuries, but fragments will be reduced. Doors may be propelled into rooms, presenting serious hazards. Majority of personnel suffer serious injuries. There are likely to be a limited number (10 percent to 25 percent) of fatalities.</p> <p>Low Level of Protection – Moderate damage, unrepairable. Major deformation of non-structural elements and secondary structural members and minor deformation of primary structural members, but progressive collapse is unlikely. Glazing will break, but fall within 1 meter of the wall or otherwise not present a significant fragment hazard. Doors may fail, but they will rebound out of their frames, presenting minimal hazards. Majority of personnel suffer significant injuries. There may be a few (&lt;10 percent) fatalities.</p> <p>Medium Level Protection – Minor damage, repairable. Minor deformations of non-structural elements and secondary structural members and no permanent deformation in primary structural members. Glazing will break, but will remain in the window frame. Doors will stay in frames, but will not be reusable. Some minor</p>	

Section	Vulnerability Questions	Guidance	Observations
		<p>injuries, but fatalities are unlikely.                      High Level Protection – Minimal damage, repairable. No permanent deformation of primary and secondary structural members or non-structural elements. Glazing will not break. Doors will be reusable. Only superficial injuries are likely.                      Reference: <i>DoD UFC 4-010-01</i></p>	
3.6	<p>Is the structure vulnerable to progressive collapse?</p> <p>Is the building capable of sustaining the removal of a column for one floor above grade at the building perimeter without progressive collapse?</p> <p>In the event of an internal explosion in an uncontrolled public ground floor area does the design prevent progressive collapse due to the loss of one primary column?</p> <p>Do architectural or structural features provide a minimum 6-inch stand-off to the internal columns (primary vertical load carrying members)?</p> <p>Are the columns in the unscreened internal spaces designed for an unbraced length equal to two floors, or three floors where there are two levels of parking?</p>	<p>Design to mitigate progressive collapse is an independent analysis to determine a system’s ability to resist structural collapse upon the loss of a major structural element or the system’s ability to resist the loss of a major structural element. Design to mitigate progressive collapse may be based on the methods outlined in ASCE 7-98 (now 7-02). Designers may apply static and/or dynamic methods of analysis to meet this requirement and ultimate load capacities may be assumed in the analyses. Combine structural upgrades for retrofits to existing buildings, such as seismic and progressive collapse, into a single project due to the economic synergies and other cross benefits. Existing facilities may be retrofitted to withstand the design level threat or to accept the loss of a column for one floor above grade at the building perimeter without progressive collapse. Note that collapse of floors or roof must not be permitted.                      Reference: <i>GSA PBS-P100</i></p>	Unknown without a more detailed on-site assessment.

3.7	Are there adequate redundant load paths in the structure?	Special consideration should be given to materials that have inherent ductility and that are better able to respond to load reversals, such as cast in place reinforced concrete, reinforced masonry, and steel construction. Careful detailing is required for material such as pre-stressed concrete, pre-cast concrete, and masonry to adequately respond to the design loads. Primary vertical load carrying members should be protected where parking is inside a facility and the building superstructure is supported by the parking structure. Reference: <i>GSA PBS-P100</i>	Unknown without a more detailed on-site assessment.
3.8	Are there transfer girders supported by columns within unscreened public spaces or at the exterior of the building?	Transfer girders allow discontinuities in columns between the roof and foundation. This design has inherent difficulty in transferring load to redundant paths upon loss of a column or the girder. Transfer beams and girders that, if lost, may cause progressive collapse are highly discouraged. Reference: <i>GSA PBS-P100</i>	Unknown without a more detailed on-site assessment.
3.9	What is the grouting and reinforcement of masonry (brick and/or concrete masonry unit (CMU)) exterior walls?	Avoid unreinforced masonry exterior walls. Reinforcement can run the range of light to heavy, depending upon the stand-off distance available and postulated design threat. Reference: <i>GSA PBS-P100</i> recommends fully grouted and reinforced CMU construction where CMU is selected. Reference: <i>DoD Minimum Antiterrorism Standards for Buildings</i> states “Unreinforced masonry walls are prohibited for the exterior walls of new buildings. A minimum of 0.05 percent vertical reinforcement with a maximum spacing of 1,200 mm (48 in) will be provided. For existing buildings, implement mitigating measures to provide an equivalent level of protection.” [This is light	Unknown without a more detailed on-site assessment.

		reinforcement and based upon the recommended stand-off distance for the situation.]	
3.10	Will the loading dock design limit damage to adjacent areas and vent explosive force to the exterior of the building?	Design the floor of the loading dock for blast resistance if the area below is occupied or contains critical utilities. Reference: <i>GSA PBS-P100</i>	
3.11	Are mailrooms, where packages are received and opened for inspection, and unscreened retail spaces designed to mitigate the effects of a blast on primary vertical or lateral bracing members?	Where mailrooms and unscreened retail spaces are located in occupied areas or adjacent to critical utilities, walls, ceilings, and floors, they should be blast- and fragment- resistant. Methods to facilitate the venting of explosive forces and gases from the interior spaces to the outside of the structure may include blow-out panels and window system designs that provide protection from blast pressure applied to the outside, but that readily fail and vent if exposed to blast pressure on the inside. Reference: <i>GSA PBS-P100</i>	
<b>4</b>	<b>Building Envelope</b>		
4.1	What is the designed or estimated protection level of the exterior walls against the postulated explosive threat?	The performance of the façade varies to a great extent on the materials. Different construction includes brick or stone with block backup, steel stud walls, precast panels, or curtain wall with glass, stone, or metal panel elements. Shear walls that are essential to the lateral and vertical load bearing system and that also function as exterior walls should be considered primary structures and should resist the actual blast loads predicted from the threats specified. Where exterior walls are not designed for the full design loads, special consideration should be given to construction types that reduce the potential for injury. Reference: <i>GSA PBS-P100</i>	

<p>4.2</p>	<p>Is there less than 40 % fenestration openings per structural bay?</p> <p>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.)</p> <p>Do the glazing systems with a 1/2-inch (3/4-inch better) bite contain an application of structural silicone?</p> <p>Is the glazing laminated or is it protected with an anti-shatter (fragment retention) film?</p> <p>If an anti-shatter film is used, is it a minimum of a 7-mil thick film, or specially manufactured 4-mil thick film?</p>	<p>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.</p> <p>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).</p> <p>Reference: GSA PBS-P100</p>	
<p>4.3</p>	<p>Do the walls, anchorage, and window framing fully develop the capacity of the glazing material selected?</p> <p>Are the walls capable of withstanding the dynamic reactions from the</p>	<p>Government produced and sponsored computer programs coupled with test data and recognized dynamic structural analysis techniques may be used to determine whether the glazing either survives the specified threats or the post damage performance of the glazing protects the occupants. A</p>	<p>Unknown without a more detailed on-site assessment.</p>

	<p>windows?</p> <p>Will the anchorage remain attached to the walls of the building during an explosive event without failure?</p> <p>Is the façade connected to back-up block or to the structural frame?</p> <p>Are non-bearing masonry walls reinforced?</p>	<p>breakage probability no higher than 750 breaks per 1,000 may be used when calculating loads to frames and anchorage.</p> <p>The intent is to ensure the building envelope provides relatively equal protection against the postulated explosive threat for the walls and window systems for the safety of the occupants, especially in rooms with exterior walls.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
4.4	<p>Does the building contain ballistic glazing?</p> <p>Does the ballistic glazing meet the requirements of UL 752 Bullet-Resistant Glazing?</p> <p>Does the building contain security-glazing?</p> <p>Does the security-glazing meet the requirements of ASTM F1233 or UL 972, Burglary Resistant Glazing Material?</p> <p>Do the window assemblies containing forced entry resistant glazing (excluding the glazing) meet the requirements of ASTM F 588?</p>	<p>Glass-clad polycarbonate or laminated polycarbonate are two types of acceptable glazing material.</p> <p>If windows are upgraded to bullet-resistant, burglar-resistant, or forced entry-resistant, ensure that doors, ceilings, and floors, as applicable, can resist the same for the areas of concern.</p> <p>Reference: <i>GSA PBS-P100</i></p>	<p>Unknown without a more detailed on-site assessment.</p>
4.5	<p>Do non-window openings, such as mechanical vents and exposed plenums, provide the same level of protection required for the exterior wall?</p>	<p>In-filling of blast over-pressures must be considered through non-window openings such that structural members and all mechanical system mountings and attachments should resist these interior fill pressures.</p>	<p>Unknown without a more detailed on-site assessment.</p>

		<p>These non-window openings should also be as secure as the rest of the building envelope against forced entry. Reference: <i>GSA PBS-P100</i></p>	
<b>6</b>	<b>Mechanical Systems (HVAC and CBR)</b>		
6.1	<p>Where are the air intakes and exhaust louvers for the building? (low, high, or midpoint of the building structure)</p> <p>Are the intakes and exhausts accessible to the public?</p>	<p>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 the throwing of anything into the enclosure near the intakes. Reference: <i>GSA PBS-P100</i> states that air intakes should be on the fourth floor or higher and, on buildings with three floors or less, they should be on the roof or as high as practical. Locating intakes high on a wall is preferred over a roof location. Reference: <i>DoD UFC 4-010-01</i> states that, for all new inhabited buildings covered by this document, all air intakes should be located at least 3 meters (10 feet) above the ground. Reference: <i>CDC/NIOSH, Pub 2002-139</i> states: "An extension height of 12 feet (3.7 m) will place the intake out of reach of individuals without some assistance. Also, the entrance to the intake should be covered with a sloped metal mesh to reduce the threat of objects being tossed into the intake. A minimum slope of 45° is generally adequate. Extension height should be increased where existing platforms or building features (i.e., loading docks, retaining walls) might provide access to the outdoor air intakes". Reference: <i>LBNL PUB-51959</i>: Exhausts are also a concern during an outdoor release, especially if exhaust fans are not in continuous operation, due to wind effects and chimney effects (air movement due to differential temperature).</p>	

6.2	<p>Is roof access limited to authorized personnel by means of locking mechanisms?</p> <p>Is access to mechanical areas similarly controlled?</p>	<p>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.</p> <p>References: <i>GSA PBS-P100</i>, <i>CDC/NIOSH Pub 2002-139</i>, and <i>LBNL Pub 51959</i></p>	Unknown without a more detailed on-site assessment.
6.3	Are there multiple air intake locations?	<p>Single air intakes may feed several air handling units. Indicate if the air intakes are localized or separated. Installing low-leakage dampers is one way to provide the system separation when necessary.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
6.4	<p>What are the types of air filtration? Include the efficiency and number of filter modules for each of the main air handling systems.</p> <p>Is there any collective protection for chemical, biological, and radiological contamination designed into the building?</p>	<p>MERV – Minimum Efficiency Reporting Value          HEPA – High Efficiency Particulate Air          Activated charcoal for gases          Ultraviolet C for biologicals          Consider mix of approaches for optimum protection and cost-effectiveness.</p> <p>Reference: <i>CDC/NIOSH Pub 2002-139</i></p>	
6.5	Is there space for larger filter assemblies on critical air handling systems?	<p>Air handling units serving critical functions during continued operation may be retrofitted to provide enhanced protection during emergencies. However, upgraded filtration may have negative effects upon the overall air handling system operation, such as increased pressure drop.</p> <p>Reference: <i>CDC/NIOSH Pub 2002-139</i></p>	Unknown without a more detailed on-site assessment.
6.6	Are there provisions for air monitors or sensors for	Duct mounted sensors are usually found in limited cases in laboratory areas. Sensors	Unknown without a more detailed on-site assessment.

	chemical or biological agents?	generally have a limited spectrum of high reliability and are costly. Many different technologies are undergoing research to provide capability. Reference: <i>CDC/NIOSH Pub 2002-139</i>	
6.7	By what method are air intakes and exhausts closed when not operational?	Motorized (low-leakage, fast-acting) dampers are the preferred method for closure with fail-safe to the closed position so as to support in-place sheltering. References: <i>CDC/NIOSH Pub 2002-139 and LBNL Pub 51959</i>	Unknown without a more detailed on-site assessment.
6.8	How are air handling systems zoned?  What areas and functions do each of the primary air handling systems serve?	Understanding the critical areas of the building that must continue functioning focuses security and hazard mitigation measures. Applying HVAC zones that isolate lobbies, mailrooms, loading docks, and other entry and storage areas from the rest of the building HVAC zones and maintaining negative pressure within these areas will contain CBR releases. Identify common return systems that service more than one zone, effectively making a large single zone. Conversely, emergency egress routes should receive positive pressurization to ensure contamination does not hinder egress. Consider filtering of the pressurization air. References: <i>CDC/NIOSH Pub 2002-139 and LBNL Pub 51959</i>	Unknown without a more detailed on-site assessment.
6.9	Are there large central air handling units or are there multiple units serving separate zones?	Independent units can continue to operate if damage occurs to limited areas of the building. Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
6.10	Are there any redundancies in the air handling system?  Can critical areas be served from other units if	Redundancy reduces the security measures required compared to a non-redundant situation. Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	Unknown without a more detailed on-site assessment.

	a major system is disabled?		
6.11	<p>Is the air supply to critical areas compartmentalized?</p> <p>Similarly, are the critical areas or the building as a whole, considered tight with little or no inleakage?</p>	<p>During chemical, biological, and radiological situations, the intent is to either keep the contamination localized in the critical area or prevent its entry into other critical, non-critical, or public areas. Systems can be cross-connected through building openings (doorways, ceilings, partial wall), ductwork leakage, or pressure differences in air handling system. In standard practice, there is almost always some air carried between ventilation zones by pressure imbalances, due to elevator piston action, chimney effect, and wind effects.</p> <p>Smoke testing of the air supply to critical areas may be necessary.</p> <p>References: <i>CDC/NIOSH Pub 2002-139 and LBNL Pub 51959</i></p>	Unknown without a more detailed on-site assessment.
6.12	<p>Are supply, return, and exhaust air systems for critical areas secure?</p> <p>Are all supply and return ducts completely connected to their grilles and registers and secure?</p> <p>Is the return air not ducted?</p>	<p>The air systems to critical areas should be inaccessible to the public, especially if the ductwork runs through the public areas of the building. It is also more secure to have a ducted air handling system versus sharing hallways and plenums above drop ceilings for return air. Non-ducted systems provide greater opportunity for introducing contaminants.</p> <p>References: <i>CDC/NIOSH Pub 2002-139 and LBNL Pub 51959</i></p>	Unknown without a more detailed on-site assessment.
6.13	<p>What is the method of temperature and humidity control?</p> <p>Is it localized or centralized?</p>	<p>Central systems can range from monitoring only to full control. Local control may be available to override central operation. Of greatest concern are systems needed before, during, and after an incident that may be unavailable due to temperature and humidity exceeding operational limits (e.g., main telephone switch room).</p> <p>Reference: <i>DOC CIAO</i></p>	

		<i>Vulnerability Assessment Framework 1.1</i>	
6.14	<p>Where are the building automation control centers and cabinets located?</p> <p>Are they in secure areas?</p> <p>How is the control wiring routed?</p>	<p>Access to any component of the building automation and control system could compromise the functioning of the system, increasing vulnerability to a hazard or precluding their proper operation during a hazard incident.</p> <p>The HVAC and exhaust system controls should be in a secure area that allows rapid shutdown or other activation based upon location and type of attack.</p> <p>References: <i>FEMA 386-7, DOC CIAO Vulnerability Assessment Framework 1.1 and LBNL Pub 51959</i></p>	Unknown without a more detailed on-site assessment.
6.15	<p>Does the control of air handling systems support plans for sheltering in place or other protective approach?</p>	<p>The micro-meteorological effects of buildings and terrain can alter travel and duration of chemical agents and hazardous material releases. Shielding in the form of sheltering in place can protect people and property from harmful effects.</p> <p>To support in-place sheltering, the air handling systems require the ability for authorized personnel to rapidly turn off all systems. However, if the system is properly filtered, then keeping the system operating will provide protection as long as the air handling system does not distribute an internal release to other portions of the building.</p> <p>Reference: <i>CDC/NIOSH Pub 2002-139</i></p>	Unknown without a more detailed on-site assessment.
6.16	<p>Are there any smoke evacuation systems installed?</p> <p>Does it have purge capability?</p>	<p>For an internal blast, a smoke removal system may be essential, particularly in large, open spaces. The equipment should be located away from high-risk areas, the system controls and wiring should be protected, and it should be connected to emergency power. This exhaust capability can be built into areas with significant risk on internal events, such as</p>	

		lobbies, loading docks, and mailrooms. Consider filtering of the exhaust to capture CBR contaminants. References: <i>GSA PBS-P100, CDC/NIOSH Pub 2002-139, and LBNL Pub 51959</i>	
6.17	Where is roof-mounted equipment located on the roof? (near perimeter, at center of roof)	Roof-mounted equipment should be kept away from the building perimeter. Reference: <i>U.S. Army TM 5-853</i>	Unknown without a more detailed on-site assessment.
6.18	Are fire dampers installed at all fire barriers?  Are all dampers functional and seal well when closed?	All dampers (fire, smoke, outdoor air, return air, bypass) must be functional for proper protection within the building during an incident. Reference: <i>CDC/NIOSH Pub 2002-139</i>	
6.19	Do fire walls and fire doors maintain their integrity?	The tightness of the building (both exterior, by weatherization to seal cracks around doors and windows, and internal, by zone ducting, fire walls, fire stops, and fire doors) provides energy conservation benefits and functional benefits during a CBR incident. Reference: <i>LBNL Pub 51959</i>	Unknown without a more detailed on-site assessment.
6.20	Do elevators have recall capability and elevator emergency message capability?	Although a life-safety code and fire response requirement, the control of elevators also has benefit during a CBR incident. The elevators generate a piston effect, causing pressure differentials in the elevator shaft and associated floors that can force contamination to flow up or down. Reference: <i>LBNL Pub 51959</i>	
6.21	Is access to building information restricted?	Information on building operations, schematics, procedures, plans, and specifications should be strictly controlled and available only to authorized personnel. References: <i>CDC/NIOSH Pub 2002-139 and LBNL Pub 51959</i>	

6.22	Does the HVAC maintenance staff have the proper training, procedures, and preventive maintenance schedule to ensure CBR equipment is functional?	Functional equipment must interface with operational procedures in an emergency plan to ensure the equipment is properly operated to provide the protection desired. The HVAC system can be operated in different ways, depending upon an external or internal release and where in the building an internal release occurs. Thus maintenance and security staff must have the training to properly operate the HVAC system under different circumstances, even if the procedure is to turn off all air movement equipment. Reference: <i>CDC/NIOSH Pub 2002-139 and LBNL Pub 51959</i>	Unknown without a more detailed on-site assessment.
<b>7</b>	<b>Plumbing and Gas Systems</b>		
7.1	What is the method of water distribution?	Central shaft locations for piping are more vulnerable than multiple riser locations. Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	Unknown without a more detailed on-site assessment.
7.2	What is the method of gas distribution? (heating, cooking, medical, process)	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	Unknown without a more detailed on-site assessment.
7.3	Is there redundancy to the main piping distribution?	Looping of piping and use of section valves provide redundancies in the event sections of the system are damaged. Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	Unknown without a more detailed on-site assessment.
7.4	What is the method of heating domestic water?  What fuel(s) is used?	Single source of hot water with one fuel source is more vulnerable than multiple sources and multiple fuel types. Domestic hot water availability is an operational concern for many building occupancies. Reference: <i>Physical Security</i>	Unknown without a more detailed on-site assessment.

		<i>Assessment for the Department of Veterans Affairs Facilities</i>	
7.5	<p>Where are gas storage tanks located? (heating, cooking, medical, process)</p> <p>How are they piped to the distribution system? (above or below ground)</p>	<p>The concern is that the tanks and piping could be vulnerable to a moving vehicle or a bomb blast either directly or by collateral damage due to proximity to a higher-risk area.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	Unknown without a more detailed on-site assessment.
7.6	Are there reserve supplies of critical gases?	<p>Localized gas cylinders could be available in the event of damage to the central tank system.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	Unknown without a more detailed on-site assessment.
<b>8</b>	<b>Electrical Systems</b>		
8.1	<p>Are there any transformers or switchgears located outside the building or accessible from the building exterior?</p> <p>Are they vulnerable to public access?</p> <p>Are they secured?</p>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
8.2	What is the extent of the external building lighting in utility and service areas and at normal entryways used by the building occupants?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	Unknown without a more detailed on-site assessment.
8.3	How are the electrical rooms secured and where are they located relative to other higher risk areas, starting with the main electrical distribution room at the service entrance?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	Unknown without a more detailed on-site assessment.

<p>8.4</p>	<p>Are critical electrical systems co-located with other building systems?</p> <p>Are critical electrical systems located in areas outside of secured electrical areas?</p> <p>Is security system wiring located separately from electrical and other service systems?</p>	<p>Collocation concerns include rooms, ceilings, raceways, conduits, panels, and risers. Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
<p>8.5</p>	<p>How are electrical distribution panels serving branch circuits secured or are they in secure locations?</p>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	<p>Unknown without a more detailed on-site assessment.</p>
<p>8.6</p>	<p>Does emergency backup power exist for all areas within the building or for critical areas only?</p> <p>How is the emergency power distributed?</p> <p>Is the emergency power system independent from the normal electrical service, particularly in critical areas?</p>	<p>There should be no single critical node that allows both the normal electrical service and the emergency backup power to be affected by a single incident. Automatic transfer switches and interconnecting switchgear are the initial concerns.</p> <p>Emergency and normal electrical equipment should be installed separately, at different locations, and as far apart as possible. Reference: <i>GSA PBS-P100</i></p>	
<p>8.7</p>	<p>How is the primary electrical system wiring distributed?</p> <p>Is it co-located with other major utilities?</p>	<p>Central utility shafts may be subject to damage, especially if there is only one for the building. Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	<p>Unknown without a more detailed on-site assessment.</p>

	Is there redundancy of distribution to critical areas?		
<b>9</b>	<b>Fire Alarm Systems</b>		
9.1	<p>Is the building fire alarm system centralized or localized?</p> <p>How are alarms annunciated, both locally and centrally?</p> <p>Are critical documents and control systems located in a secure yet accessible location?</p>	<p>Fire alarm systems must first warn building occupants to evacuate for life safety. Then they must inform the responding agency to dispatch fire equipment and personnel.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
9.2	<p>Where are the fire alarm panels located?</p> <p>Do they allow access to unauthorized personnel?</p>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
9.3	<p>Is the fire alarm system stand-alone or integrated with other functions such as security and environmental or building management systems?</p> <p>What is the interface?</p>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
9.4	<p>Do key fire alarm system components have fire- and blast-resistant separation?</p>	<p>This is especially necessary for the fire command center or fire alarm control center. The concern is to similarly protect critical components as described in Items 2.19, 5.7, and 10.3.</p>	<p>Unknown without a more detailed on-site assessment.</p>
9.5	<p>Is there redundant off-premises fire alarm reporting?</p>	<p>Fire alarms can ring at a fire station, at an intermediary alarm monitoring center, or autodial</p>	

		someone else. See Items 5.21 and 10.5.	
<b>10</b>	<b>Communications and IT Systems</b>		
10.1	<p>Where is the main telephone distribution room and where is it in relation to higher risk areas?</p> <p>Is the main telephone distribution room secure?</p>	<p>One can expect to find voice, data, signal, and alarm systems to be routed through the main telephone distribution room. Reference: <i>FEMA 386-7</i></p>	
10.2	<p>Does the telephone system have an UPS (uninterruptible power supply)?</p> <p>What is its type, power rating, operational duration under load, and location? (battery, on-line, filtered)</p>	<p>Many telephone systems are now computerized and need a UPS to ensure reliability during power fluctuations. The UPS is also needed to await any emergency power coming on line or allow orderly shutdown. Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i></p>	<p>Unknown without a more detailed on-site assessment.</p>
10.3	<p>Where are communication systems wiring closets located? (voice, data, signal, alarm)</p> <p>Are they co-located with other utilities?</p> <p>Are they in secure areas?</p>	<p>Concern is to have separation distance from other utilities and higher-risk areas to avoid collateral damage. Security approaches on the closets include door alarms, closed circuit television, swipe cards, or other logging notifications to ensure only authorized personnel have access to these closets. Reference: <i>FEMA 386-7</i></p>	<p>Unknown without a more detailed on-site assessment.</p>
10.4	<p>How is communications system wiring distributed? (secure chases and risers, accessible public areas)</p>	<p>The intent is to prevent tampering with the systems. Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	<p>Unknown without a more detailed on-site assessment.</p>
10.5	<p>Are there redundant communications systems available?</p>	<p>Critical areas should be supplied with multiple or redundant means of communications. Power outage phones can provide redundancy</p>	

		as they connect directly to the local commercial telephone switch off site and not through the building telephone switch in the main telephone distribution room. A base radio communication system with antenna can be installed in stairwells, and portable sets distributed to floors. References: <i>GSA PBS-P100 and FEMA 386-7</i>	
10.6	<p>Where are the main distribution facility, data centers, routers, firewalls, and servers located and are they secure?</p> <p>Where are the secondary and/or intermediate distribution facilities and are they secure?</p>	<p>Concern is collateral damage from manmade hazards and redundancy of critical functions. Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i></p>	
10.7	<p>What type and where are the WAN (wide area network) connections?</p>	<p>Critical facilities should have two Minimum-Points-of-Presence (MPOPs) where the telephone company's outside cable terminates inside the building. It is functionally a service entrance connection that demarcates where the telephone company's property stops and the building owner's property begins. The MPOPs should not be collocated and they should connect to different telephone company central offices so that the loss of one cable or central office does not reduce capability. Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	<p>Unknown without a more detailed on-site assessment.</p>
10.8	<p>What type, power rating, and location of the UPS (uninterruptible power supply)? (battery, on-line, filtered)</p>	<p>Consider that UPS should be found at all computerized points from the main distribution facility to individual data closets and at critical personal computers/terminals.</p>	

	Are the UPS also connected to emergency power?	Critical LAN sections should also be on backup power. Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i>	
10.9	What type of LAN (local area network) cabling and physical topology is used? (Category (Cat) 5, Gigabit Ethernet, Ethernet, Token Ring)	The physical topology of a network is the way in which the cables and computers are connected to each other. The main types of physical topologies are: Bus (single radial where any damage on the bus affects the whole system, but especially all portions downstream) Star (several computes are connected to a hub and many hubs can be in the network – the hubs can be critical nodes, but the other hubs continue to function if one fails) Ring (a bus with a continuous connection - least used, but can tolerate some damage because if the ring fails at a single point it can be rerouted much like a looped electric or water system) The configuration and the availability of surplus cable or spare capacity on individual cables can reduce vulnerability to hazard incidents. Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	Unknown without a more detailed on-site assessment.
10.10	For installed radio/wireless systems, what are their types and where are they located? (RF (radio frequency), HF (high frequency), VHF (very high frequency), MW (medium wave))	Depending upon the function of the wireless system, it could be susceptible to accidental or intended jamming or collateral damage. Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	Unknown without a more detailed on-site assessment.
10.11	Do the IT (Information Technology – computer) systems meet requirements of confidentiality, integrity,	Ensure access to terminals and equipment for authorized personnel only and ensure system up-time to meet operational needs. Reference: <i>DOC CIAO</i>	

	and availability?	<i>Vulnerability Assessment Framework 1.1</i>	
10.12	Where is the disaster recovery/mirroring site?	A site with suitable equipment that allows continuation of operations or that mirrors (operates in parallel to) the existing operation is beneficial if equipment is lost during a natural or manmade disaster. The need is based upon the criticality of the operation and how quickly replacement equipment can be put in place and operated. Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i>	
10.13	Where is the back-up tape/file storage site and what is the type of safe environment? (safe, vault, underground)  Is there redundant refrigeration in the site?	If equipment is lost, data are most likely lost, too. Backups are needed to continue operations at the disaster recovery site or when equipment can be delivered and installed. Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i>	Unknown without a more detailed on-site assessment.
10.14	Are there any SATCOM (satellite communications) links? (location, power, UPS, emergency power, spare capacity/capability)	SATCOM links can serve as redundant communications for voice and data if configured to support required capability after a hazard incident. Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i>	Unknown without a more detailed on-site assessment.
10.15	Is there a mass notification system that reaches all building occupants? (public address, pager, cell phone, computer override, etc.)  Will one or more of these systems be operational under hazard conditions? (UPS, emergency power)	Depending upon building size, a mass notification system will provide warning and alert information, along with actions to take before and after an incident if there is redundancy and power. Reference: <i>DoD UFC 4-010-01</i>	

10.16	<p>Do control centers and their designated alternate locations have equivalent or reduced capability for voice, data, mass notification, etc.? (emergency operations, security, fire alarms, building automation)</p> <p>Do the alternate locations also have access to backup systems, including emergency power?</p>	Reference: <i>GSA PBS-P100</i>	
<b>11</b>	<b>Equipment Operations and Maintenance</b>		
11.1	<p>Are there composite drawings indicating location and capacities of major systems and are they current? (electrical, mechanical, and fire protection; and date of last update)</p> <p>Do updated O&amp;M (operation and maintenance) manuals exist?</p>	<p>Within critical infrastructure protection at the building level, the current configuration and capacity of all critical systems must be understood to ensure they meet emergency needs. Manuals must also be current to ensure operations and maintenance keeps these systems properly functioning. The system must function during an emergency unless directly affected by the hazard incident. Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	Unknown without a more detailed on-site assessment.
11.2	<p>Have critical air systems been rebalanced?</p> <p>If so, when and how often?</p>	<p>Although the system may function, it must be tested periodically to ensure it is performing as designed. Balancing is also critical after initial construction to set equipment to proper performance per the design. Rebalancing may only occur during renovation. Reference: <i>CDC/NIOSH Pub 2002-139</i></p>	Unknown without a more detailed on-site assessment.
11.3	Is air pressurization monitored regularly?	Some areas require positive or negative pressure to function properly. Pressurization is critical in a hazardous environment or	Unknown without a more detailed on-site assessment.

		<p>emergency situation. Measuring pressure drop across filters is an indication when filters should be changed, but also may indicate that low pressures are developing downstream and could result in loss of expected protection. Reference: <i>CDC/NIOSH Pub 2002-139</i></p>	
11.4	Does the building have a policy or procedure for periodic recommissioning of major M/E/P (Mechanical/Electrical/Plumbing) systems?	<p>Recommissioning involves testing and balancing of systems to ascertain their capability to perform as described. Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	Unknown without a more detailed on-site assessment.
11.5	Is there an adequate operations and maintenance program including training of facilities management staff?	<p>If O&amp;M of critical systems is done with in-house personnel, management must know what needs to be done and the workforce must have the necessary training to ensure systems reliability. Reference: <i>CDC/NIOSH Pub 2002-139</i></p>	Unknown without a more detailed on-site assessment.
11.6	What maintenance and service agreements exist for M/E/P systems?	<p>When an in-house facility maintenance work force does not exist or does not have the capability to perform the work, maintenance and service contracts are the alternative to ensure critical systems will work under all conditions. The facility management staff requires the same knowledge to oversee these contracts as if the work was being done by in-house personnel. Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	Unknown without a more detailed on-site assessment.
11.7	Are backup power systems periodically tested under load?	<p>Loading should be at or above maximum connected load to ensure available capacity and automatic sensors should be tested at least once per year. Periodically (once a year as a minimum) check the duration of capacity of backup systems by</p>	Unknown without a more detailed on-site assessment.

		running them for the expected emergency duration or estimating operational duration through fuel consumption, water consumption, or voltage loss. Reference: <i>FEMA 386-7</i>	
11.8	Is stairway and exit sign lighting operational?	The maintenance program for stairway and exit sign lighting (all egress lighting) should ensure functioning under normal and emergency power conditions. Expect building codes to be updated as emergency egress lighting is moved from upper walls and over doorways to floor level as heat and smoke drive occupants to crawl along the floor to get out of the building. Signs and lights mounted high have limited or no benefit when obscured. Reference: <i>FEMA 386-7</i>	
<b>13</b>	<b>Security Master Plan</b>		
13.1	Does a written security plan exist for this site or building?  When was the initial security plan written and last revised?  Who is responsible for preparing and reviewing the security plan?	The development and implementation of a security master plan provides a roadmap that outlines the strategic direction and vision, operational, managerial, and technological mission, goals, and objectives of the organization's security program. Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i>	
13.2	Has the security plan been communicated and disseminated to key management personnel and departments?	The security plan should be part of the building design so that the construction or renovation of the structure integrates with the security procedures to be used during daily operations. Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	Unknown without a more detailed on-site assessment.
13.3	Has the security plan been	Reference: <i>Physical Security Assessment for the Department of</i>	Unknown without a more detailed on-site

	benchmarked or compared against related organizations and operational entities?	<i>Veterans Affairs Facilities</i>	assessment.
13.4	Has the security plan ever been tested and evaluated from a cost-benefit and operational efficiency and effectiveness perspective?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	Unknown without a more detailed on-site assessment.
13.5	Does it define mission, vision, short-long term security program goals and objectives?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	Unknown without a more detailed on-site assessment.
13.6	Are threats, vulnerabilities, risks adequately defined and security countermeasures addressed and prioritized relevant to their criticality and probability of occurrence?	Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i>	Unknown without a more detailed on-site assessment.
13.7	Has a security implementation schedule been established to address recommended security solutions?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	Unknown without a more detailed on-site assessment.
13.8	Have security operating and capital budgets been addressed, approved and established to support the plan?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	Unknown without a more detailed on-site assessment.
13.9	What regulatory or industry guidelines/standards were followed in the preparation of the security plan?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	Unknown without a more detailed on-site assessment.
13.10	Does the security plan address existing security	Reference: <i>Physical Security Assessment for the Department of</i>	Unknown without a more detailed on-site

	conditions from an administrative, operational, managerial and technical security systems perspective?	<i>Veterans Affairs Facilities</i>	assessment.
13.11	Does the security plan address the protection of people, property, assets, and information?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	Unknown without a more detailed on-site assessment.
13.12	Does the security plan address the following major components: access control, surveillance, response, building hardening and protection against biological, chemical, radiological and cyber-network attacks?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	Unknown without a more detailed on-site assessment.
13.13	Has the level of risk been identified and communicated in the security plan through the performance of a physical security assessment?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	Unknown without a more detailed on-site assessment.
13.14	When was the last security assessment performed?  Who performed the security risk assessment?	Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i>	Unknown without a more detailed on-site assessment.
13.15	Were the following areas of security analysis addressed in the security master plan:  Asset Analysis: Does the security plan identify and prioritize the assets to be protected in accordance to their location, control, current value, and	This process is the input to the building design and what mitigation measures will be included in the facility project to reduce risk and increase safety of the building and people. Reference: <i>USA TM 5-853, Security Engineering</i>	Unknown without a more detailed on-site assessment.

---

	<p>replacement value?</p> <p>Threat Analysis: Does the security plan address potential threats; causes of potential harm in the form of death, injury, destruction, disclosure, interruption of operations, or denial of services? (possible criminal acts (documented and review of police/security incident reports) associated with forced entry, bombs, ballistic assault, biochemical and related terrorist tactics, attacks against utility systems infrastructure and buildings)</p> <p>Vulnerability Analysis: Does the security plan address other areas and anything else associated with a site or building and its operations that can be taken advantage of to carry out a threat? (architectural design and construction of new and existing buildings, technological support systems (e.g. heating, air conditioning, power, lighting and security systems, etc.) and operational procedures, policies and controls)</p> <p>Risk Analysis: Does the security plan address the findings from the asset, threat, and vulnerability</p>		
--	---	--	--

---

	analyses to develop, recommend and consider implementation of appropriate security countermeasures?		
--	---	--	--

**Building Design Mitigation Measures**

<b>Asset-Threat/Hazard Pair</b>	<b>Current Risk Rating</b>	<b>Suggested Mitigation Measure</b>	<b>Revised Risk Rating</b>

## Unit X

---

**COURSE TITLE**

Building Design for Homeland Security

---

**UNIT TITLE**

Electronic Security Systems

---

**OBJECTIVES**

1. Use the assessment process to identify electronic security system requirements that are needed to mitigate vulnerabilities
  2. Describe the electronic security system concepts and practices that warrant special attention to enhance public safety
  3. Explain the basic concepts of electronic security system components, their capabilities, and their interaction with other systems
  4. Justify selection of electronic security systems to mitigate vulnerabilities
- 

**SCOPE**

The following topics will be covered in this unit:

1. Control centers and building management systems
  2. Perimeter layout and zoning of sensors
  3. Intrusion detection systems and sensor technologies
  4. Entry-control systems and electronic entry control technologies
  5. Closed circuit television and data-transmission media
  6. Definitions of the degree of security and control
- 

**REFERENCES**

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, pages 3-47 to 3-50; Appendix D; and Security Systems and Security Master Plan sections of Checklist at end of Chapter 1 (pages 1-81 and 1-92)
  2. Case Study – Hazardville Information Company
-

---

**This page intentionally left blank**

### UNIT X CASE STUDY ACTIVITY: ELECTRONIC SECURITY SYSTEMS

In this Unit, the emphasis will be upon the various components and technology available for use in electronic security systems. The **Building Vulnerability Assessment Checklist in FEMA 426** can be used as a screening tool for preliminary building design vulnerability assessment.

#### Requirement

Refer to the HIC case study and to the GIS portfolio to determine answers to the questions. Then review results to identify vulnerabilities and possible mitigation measures.

1. Complete the following components of the Building Vulnerability Assessment Checklist that address security systems
2. Upon completion of these portions of the checklist, refer back to the risk ratings determined in Unit VI Case Study Activity and, based on this detailed analysis, decide if the rating is accurate.
3. Select mitigation measures to reduce vulnerability and associated risk from security system design.
4. Estimate the new risk ratings for high risk asset-threat pairs based on the recommended mitigation measures.

Section	Vulnerability Questions	Guidance	Observations
12.1	<p>Are black/white or color CCTV (closed circuit television) cameras used?</p> <p>Are they monitored and recorded 24 hours/7 days a week? By whom?</p> <p>Are they analog or digital by design?</p> <p>What are the number of fixed, wireless and pan-tilt-zoom cameras used?</p> <p>Who are the manufacturers of the CCTV cameras?</p> <p>What is the age of the CCTV cameras in use?</p>	<p>Security technology is frequently considered to complement or supplement security personnel forces and to provide a wider area of coverage. Typically, these physical security elements provide the first line of defense in deterring, detecting, and responding to threats and reducing vulnerabilities. They must be viewed as an integral component of the overall security program. Their design, engineering, installation, operation, and management must be able to meet daily security challenges from a cost-effective and efficiency perspective. During and after an incident, the system, or its backups, should be functional per the planned design.</p>	<p>CCTV systems are used in the back parking area, including the loading dock area. The HIC security officer monitors the cameras from his desk. There is a VHS recorder. It is an older generation analog system.</p> <p>Unknown without a more detailed on-site assessment.</p>

Unit X: Electronic Security Systems

Section	Vulnerability Questions	Guidance	Observations
		Consider color CCTV cameras to view and record activity at the perimeter of the building, particularly at primary entrances and exits. A mix of monochrome cameras should be considered for areas that lack adequate illumination for color cameras. Reference: <i>GSA PBS P-100</i>	
12.2	Are the cameras programmed to respond automatically to perimeter building alarm events?  Do they have built-in video motion capabilities?		Unknown without a more detailed on-site assessment.
12.3	What type of camera housings are used and are they environmental in design to protect against exposure to heat and cold weather elements?		
12.4	Are panic/duress alarm buttons or sensors used, where are they located, and are they hardwired or portable?		
12.5	Are intercom call boxes used in parking areas or along the building perimeter?		
12.6	What is the transmission media used to transmit camera video signals: fiber, wire line, telephone wire, coaxial, wireless?		
12.7	Who monitors the CCTV system?		
12.8	What is the quality of video images both during the day and hours of darkness?  Are infrared camera illuminators used?		
12.9	Are the perimeter cameras supported by an uninterruptible power supply, battery, or building		

Unit X: Electronic Security Systems

Section	Vulnerability Questions	Guidance	Observations
	emergency power?		
12.10	What type of exterior Intrusion Detection System (IDS) sensors are used? (electromagnetic; fiber optic; active infrared; bistatic microwave; seismic; photoelectric; ground; fence; glass break (vibration/shock); single, double, and roll-up door magnetic contacts or switches)		
12.11	Is a global positioning satellite system (GPS) used to monitor vehicles and asset movements?		

**Security System Mitigation Measures**

<b>Asset-Threat/Hazard Pair</b>	<b>Current Risk Rating</b>	<b>Suggested Mitigation Measure</b>	<b>Revised Risk Rating</b>

## Unit XI

---

**COURSE TITLE**

Building Design for Homeland Security

---

**UNIT TITLE**

Case Study

---

**OBJECTIVES**

1. Explain building security design issues to a building owner for consideration prior to a renovation or new construction.
  2. Explain the identification process to arrive at the high risk asset – threat/hazard pairs.
  3. Justify the recommended mitigation measures, explaining the benefits in reducing the risk for the high risk situations of interest.
- 

**SCOPE**

The following topics will be covered in this unit:

1. Activity: Preparation and presentation of the top three risks identified by the group, the vulnerabilities identified for these risks, and top three recommended mitigation measures to reduce vulnerability and risk. The top three risks will be prioritized as well as the top three recommended mitigation measures with rationale and justification.
- 

**REFERENCES**

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*
  2. Case Study – Hazardville Information Company
-

---

**This page intentionally left blank**

**UNIT XI CASE STUDY ACTIVITY:  
FINALIZATION AND PRESENTATION OF GROUP RESULTS**

In this activity, students work with their groups to finalize their assessments, decide on high priority risk concerns, determine appropriate mitigation measures and present findings to the class.

**Requirement**

1. Based on findings from the previous activities completed in the previous ten units, complete the following table.
2. Be prepared to present conclusions and to justify decisions to the class in a 5-7 minute presentation.

<b>Prioritized Asset-Threat/Hazard Pair</b>	<b>Requirements to Mitigate</b>	<b>Rationale</b>
Car Bomb Blast/Site and Building	Protect front entrance from car bomb blast – 82-foot stand-off  Use planters, plinth walls, landscaping  FRF film on windows or replace with laminated glass  Consider closing in overhang area	DoD Standard 1  DoD Standard 6  DoD Standard 8

---


---

---


**This page intentionally left blank**

## APPENDIX A: CASE STUDY

### HAZARDVILLE INFORMATION COMPANY (HIC)

#### INTRODUCTION

The Hazardville Information Company (HIC) is a state-of-the art information technology (IT) services company located in a major metropolitan city in a typical suburban business office park. The company's mission is to provide information technology and services support to include hosting servers, databases, applications, and other hardware and software; develop, install, and maintain software applications; provide field support IT technicians; and provide 24-hour help desk support.



**Figure 1. Hazardville Information Company (HIC)**

The Hazardville Information Company has over 20 clients and supports approximately 1,000 users and 100 applications as a primary data center and as a disaster recovery backup site. HIC clients include local and regional government offices and commercial entities. Many clients depend on HIC's ability to provide real time IT support, on a 24 x 7 basis. Others rely on the company's IT backup services. Major clients and support contracts include:

- Fortune 500 companies
- National and regional banks and credit unions
- A major airline
- Large prime defense contractors
- Government agencies, including one classified client

**Appendix A: Case Study**

---

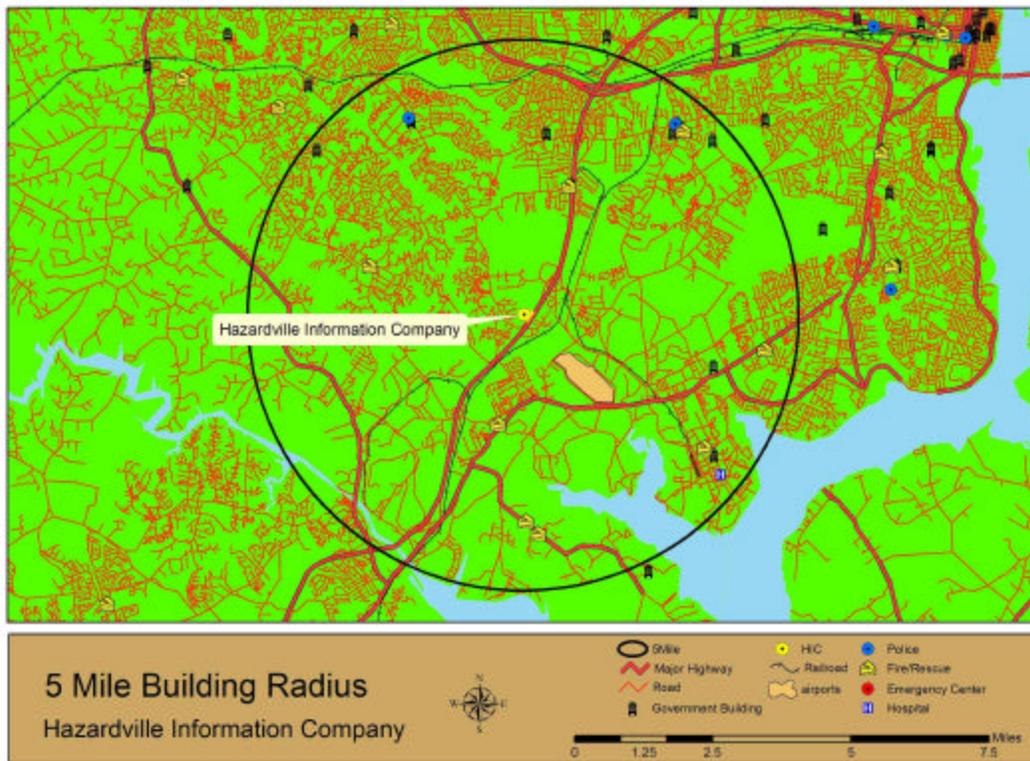
HIC is certified to provide IT support and storage to government clients at Top Secret levels, using dedicated classified equipment and networks. HIC's technology ranges from leading edge mainframe and desktop computers and optical mass storage devices to wired and wireless networks. HIC has over 130 employees and approximately 80 to 100 employees are in the building at any given time.

The Hazardville Information Company has a number of key staff that support the various projects. The president, chief executive officer, security officer, and several division managers possess high level government security clearances. Approximately half of the technical staff hold mid-level government security clearances. All company employees sign confidentiality agreements for the commercial clients and have access to a number of company's proprietary data. The IT division manager and his staff of database administrators have full administrative privileges on all systems. The company has a robust recall system and staff notification process in the event of an emergency and/or surge support requirement.

The HIC building is strategically located near many of HIC's clients and management does not want to move from the facility or location.

**GENERAL SITE DATA**

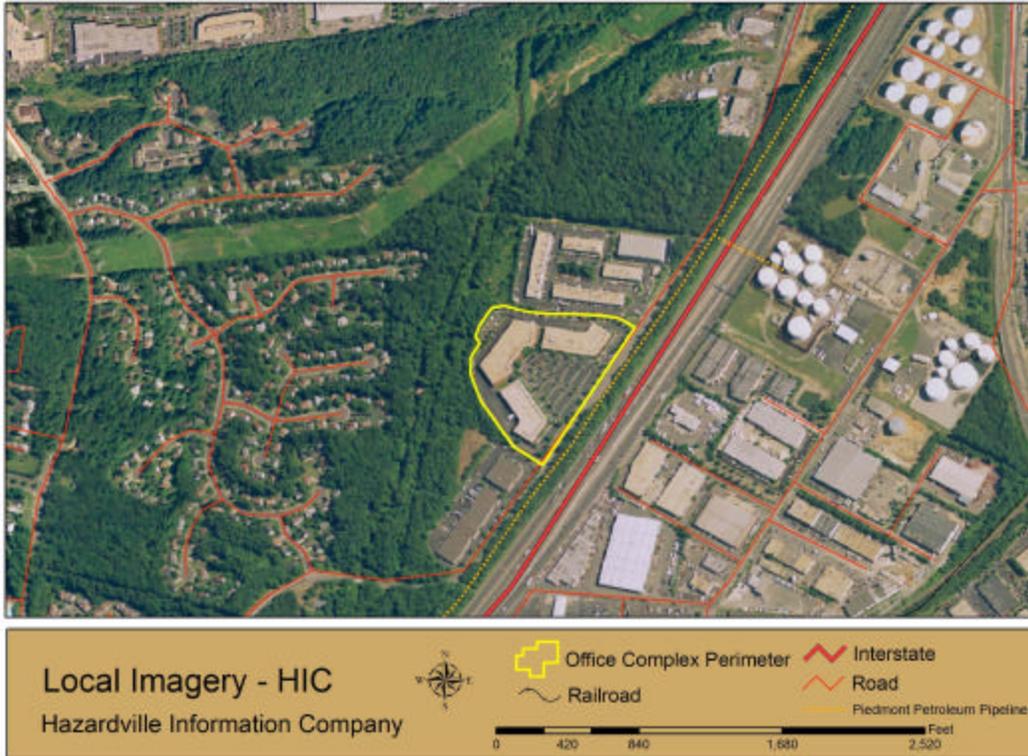
The Hazardville Information Company is located approximately 15 miles outside of a major urban city in the suburbs, and adjacent to a major interstate highway. There are several commercial iconic properties, one military installation, and several government offices within a 5-mile radius of the HIC building.



**Figure 2. HIC Corporate Business Park 5-Mile Radius**

The office building is part of a corporate business park. HIC does not control the front parking area, signage, or other general site conditions such as stormwater drainage, lighting, or vehicle and pedestrian traffic flow and movement. Front parking spots are approximately 44 feet from the main HIC lobby entrance. The business park is responsible for grounds maintenance, including cutting the grass, planting flowers, trimming trees, sweeping the parking lot, and towing unauthorized vehicles. Trash service is the responsibility of tenants. HIC has a large dumpster located at the rear of the loading dock area approximately 50 feet from the building. HIC receives the mail and packages at the front office lobby desk. Large packages and equipment are delivered to the rear loading dock. HIC does not have a separate mail room, but does have an internal administrative space with copiers, printers, supplies, and staff mailboxes. The front desk receptionist is responsible for sorting and screening all mail.

The business park is adjacent to a major interstate highway and there are a number of storage tanks, manufacturing and production facilities, and other commercial properties across the interstate.



**Figure 3. HIC Business Park Perimeter and Surrounding Buildings**

The HIC office space has client and staff parking in the front and a rear parking and loading dock area for supply trucks, vendors, and trash.

The front parking area is unrestricted, but the back parking area is fully enclosed with chain link fencing on the perimeter of the property. There is no gate or means to prevent vehicles from transiting around the rear of the business park.



**Figure 4. HIC Office Location**

There are a significant number of hazardous waste sites in near proximity to the HIC building. The vast majority are small generators such as gas stations, dry cleaning, and other commercial businesses. Large generators include the petroleum storage and production facility located across the interstate.

Appendix A: Case Study

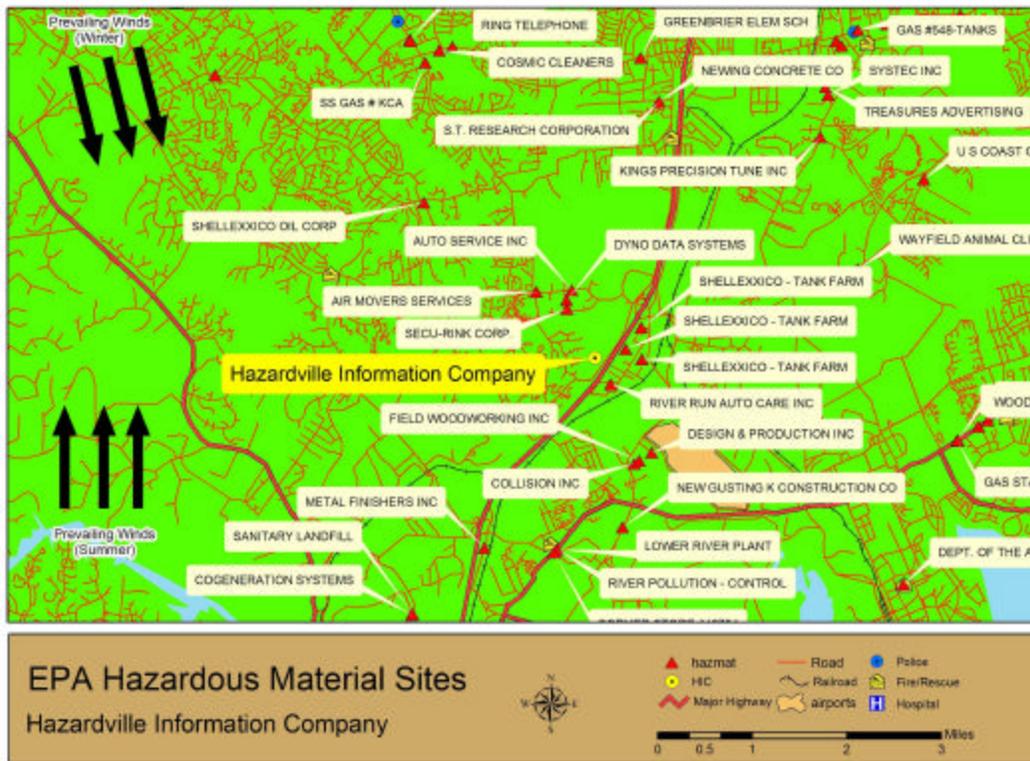


Figure 5. HAZMAT Sites Near the HIC Building

The prevailing weather pattern in the summer and fall is from the south Atlantic and the Gulf of Mexico. Warm, moist air brings thunderstorms and higher humidity. In the fall, cooler air from the north and west returns. Winter weather blasts across the state from the northern or central part of the continent. With no other weather activity, the prevailing wind is normally from the west-northwest.

The local emergency response capabilities include primary police, fire, and medical facilities approximately 8 to 10 miles away. There are multiple means of ingress and egress to the HIC building complex and the site is served by fire mains with a hydrant located approximately 200 feet from the HIC office.

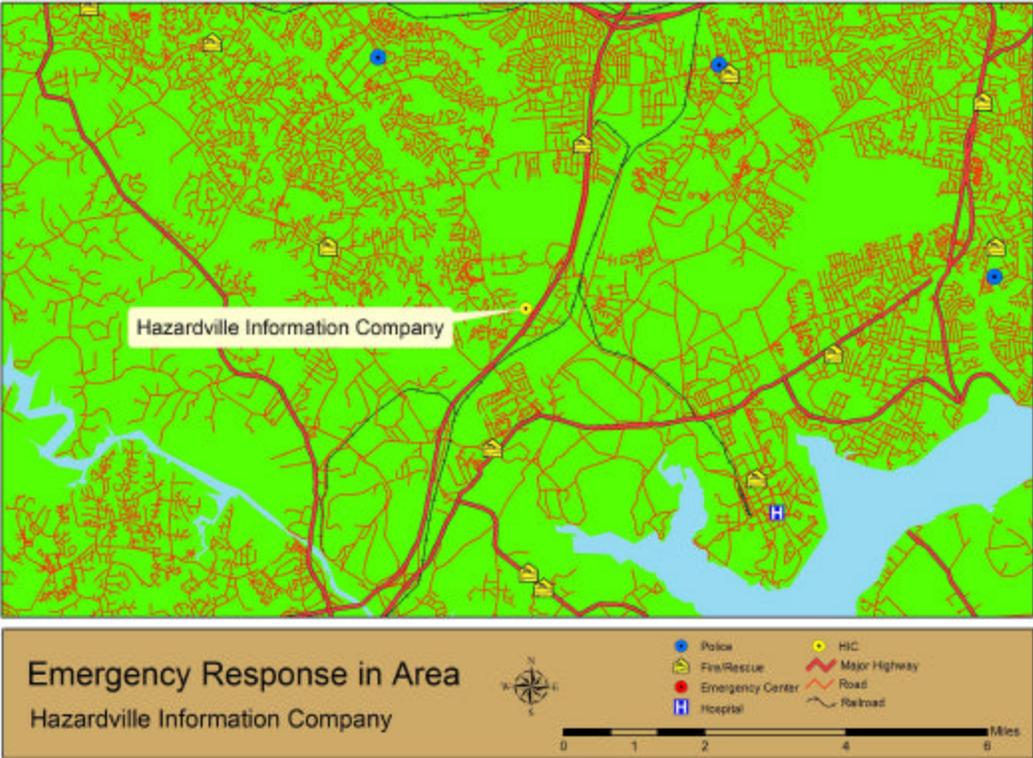
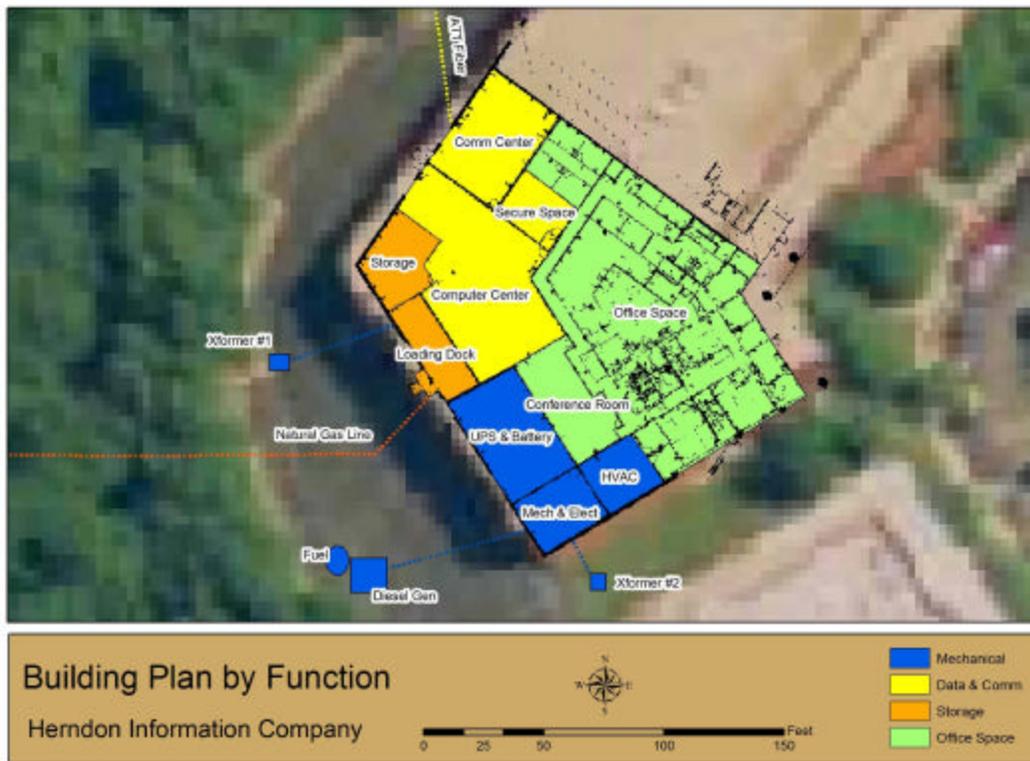


Figure 6. Emergency Response Capability Near the HIC Building



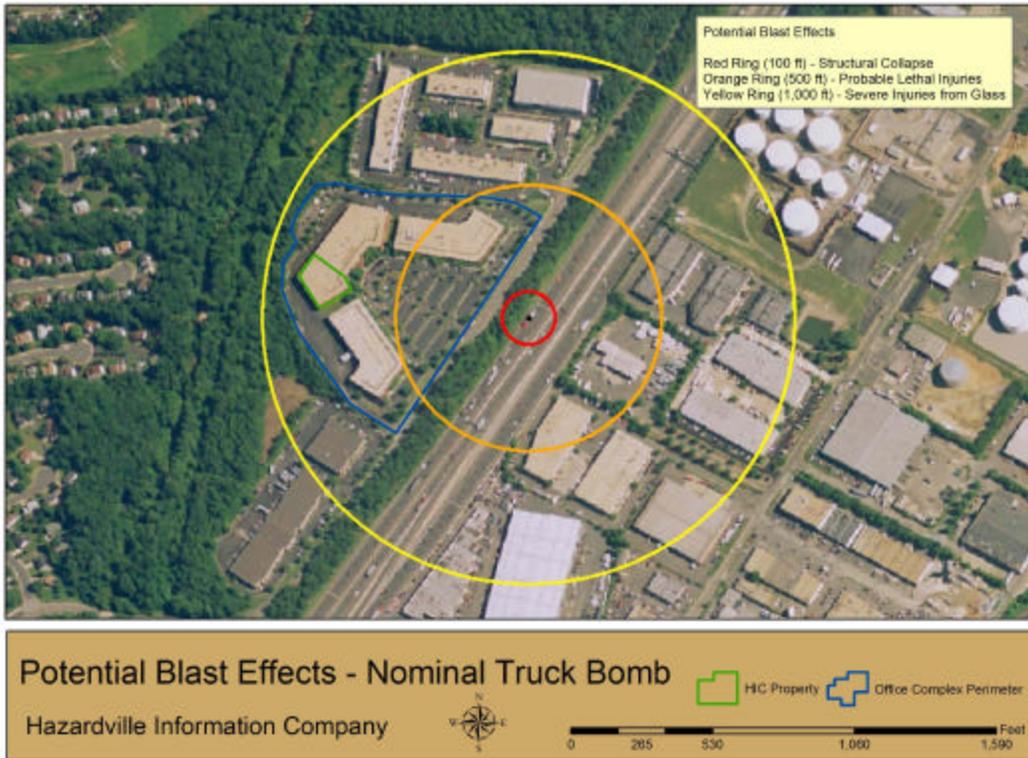
**Figure 7. HIC Functions and Building Layout**

The nominal range to effects chart radius of influence of a small car bomb detonation at the front entrance indicates that the building would experience significant damage, but likely not suffer progressive collapse. The front façade of the building is approximately 75 percent annealed glass and has an 8-foot overhang. The terrain slopes upward from the parking lot to the main entrance, and is landscaped with flower beds and trees. Key staff would probably be killed and administrative functions destroyed, but the Computer Center and Communications functions would likely survive relatively intact.



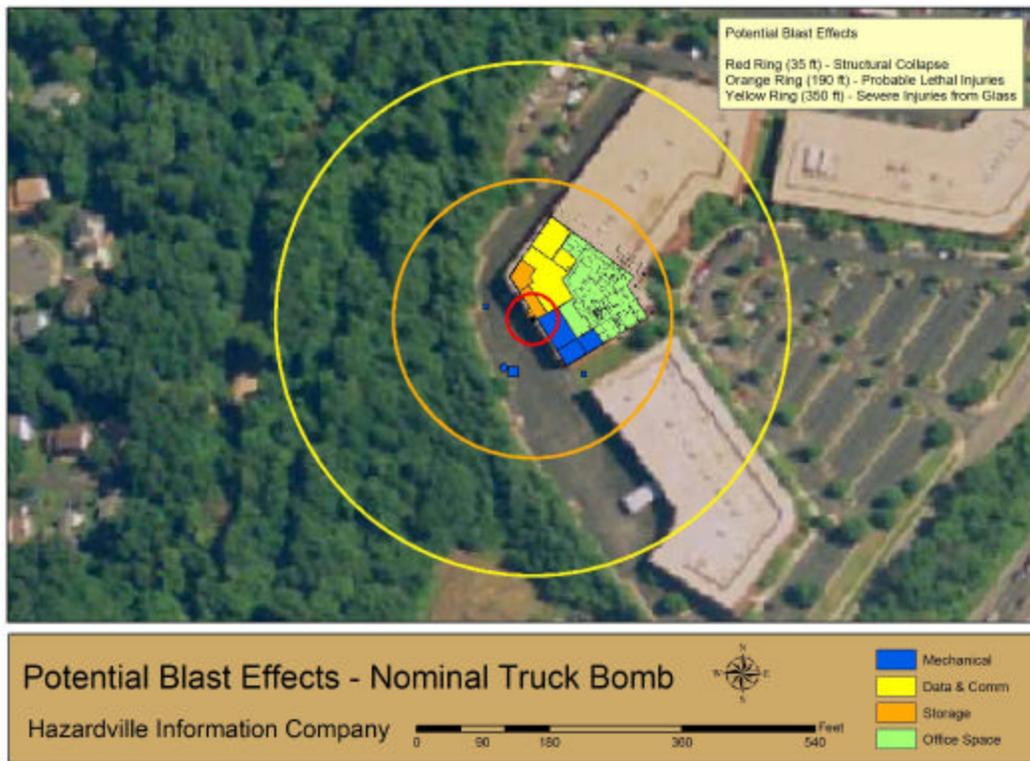
**Figure 8. Car Bomb Blast Effects (Front Entrance Parking)**

A truck bomb detonation on the interstate would also significantly damage the HIC building, primarily glass breakage and potentially some structural damage. If the truck bomb were to detonate near the tank farm, the ensuing explosion, fire, and plume would have significant impact on the HIC building.



**Figure 9. Truck Bomb Blast Effects (Interstate Highway)**

A truck bomb detonation at the rear of the HIC building at the loading dock would result in significant structural damage and potentially progressive collapse. The Computer Center, Communications, and other critical functions would be destroyed. Critical infrastructure that would be destroyed includes the mechanical/electrical room.



**Figure 10. Truck Bomb Blast Effects (Loading Dock)**

**BUILDING DATA**

The HIC Headquarters building was built in the 1980s using conventional construction techniques. The building has a 22,000-square foot main floor for offices and computers, and a 3,300-square foot executive mezzanine (a second floor over the front part of the office).

Occupancy	B, S-1
Construction Type	2C
No. of Floors	1 floor and mezzanine, high bay in rear
High Rise Code	No
Fire Suppression	Fully sprinklered, wet pipe
Floor Area	
First Floor	19,157 SF
Mezzanine	3,380 SF
Total	22,537 SF
Number of Exits	6
Exits from Mezzanine	3
Occupancy Load	
First Floor	102 occupants
Mezzanine	31 occupants

**Appendix A: Case Study**

---

Area Separation	No
Fire Alarm System	No
Monitored Sprinkler	Yes
Fence	4 feet high, rear only, to keep people from falling into a valley

**Applicable Codes**

Building	1996 BOCA National Building Code w/ 2000 VUSBC amendments
Electric	1996 VUSBC, 1996 NEC
Plumbing	1995 IPC w/1996 supplement
Mechanical	1996 International Mechanical Code
Fire	1996 BOCA National Fire Prevention Code
Accessible	1996 BOCA, 1992 CABO/ANSI 117.1

BOCA - Building Officials and Code Administrators International, Inc

USBC – Uniform Statewide Building Code

NEC – National Electric Code

IPC - International Plumbing

CABO/ANSI 117.1 – Uniform Federal Accessibility Standards

**BUILDING STRUCTURE**

The walls are made of concrete masonry units (CMUs) with a brick veneer on the outside. Steel framework supports the structure, and exposed columns are enclosed in gypsum wallboard. The roof is a metal deck with gravel on top and insulation underneath. It is slightly angled to allow water to drain. The roof overhangs the front entrance by 8 feet. This provides a covered area for employees to stay dry on rainy days. Cylindrical columns support the overhang.

Windows are double glazed, ¼-inch thick annealed glass.

With a loading dock on the west side, it is possible for vehicles to park right next to the building. Normal parking for employees is in front; the closest row is 44 feet from the front door.

The company does not have a mailroom; incoming mail is normally processed by the receptionist just inside the front door. Large packages shipped to the company (computers, etc.) are delivered to the loading dock in the rear and handled by the Computer Center staff.

**MECHANICAL SYSTEMS**

Heating for the HIC building is provided by a combination of natural gas and electricity. This provides a regulated environment for the sensitive computer and communications equipment, and a comfortable environment for employees.

The main heater sends hot air into the heating, ventilation and air conditioning (HVAC) room, next to the mechanical and electrical (M&E) room. From here it is distributed throughout the building. Offices, restrooms and the employee’s lounge are directly heated by this warm air. The

Appendix A: Case Study

Computer Center and the Communications Center use Digital Environmental Managers (DEMs) to direct the warm air where it is needed, add or remove humidity from the air, or even cool some areas while warming others.

The air used to heat or cool the HIC Headquarters building is filtered in the HVAC room using standard industrial grade MERV 8 filters. Outside make-up air is brought in through a vent in the wall located approximately 10 feet above ground level. The vent is alarmed to prevent intruder access. A screened exhaust duct is on the roof. Airflow throughout the building is through a series of ducts hidden in the ceiling of each area. The ducts are divided in half to allow them to serve as supply and return headers. The divider is insulated to minimize heat transfer from one side to the other.

The Computer Data Center has two additional air cooling units located in the data center and uses the main chill water supply. The Data Center maintains a slight net positive pressure compared to the main office areas.

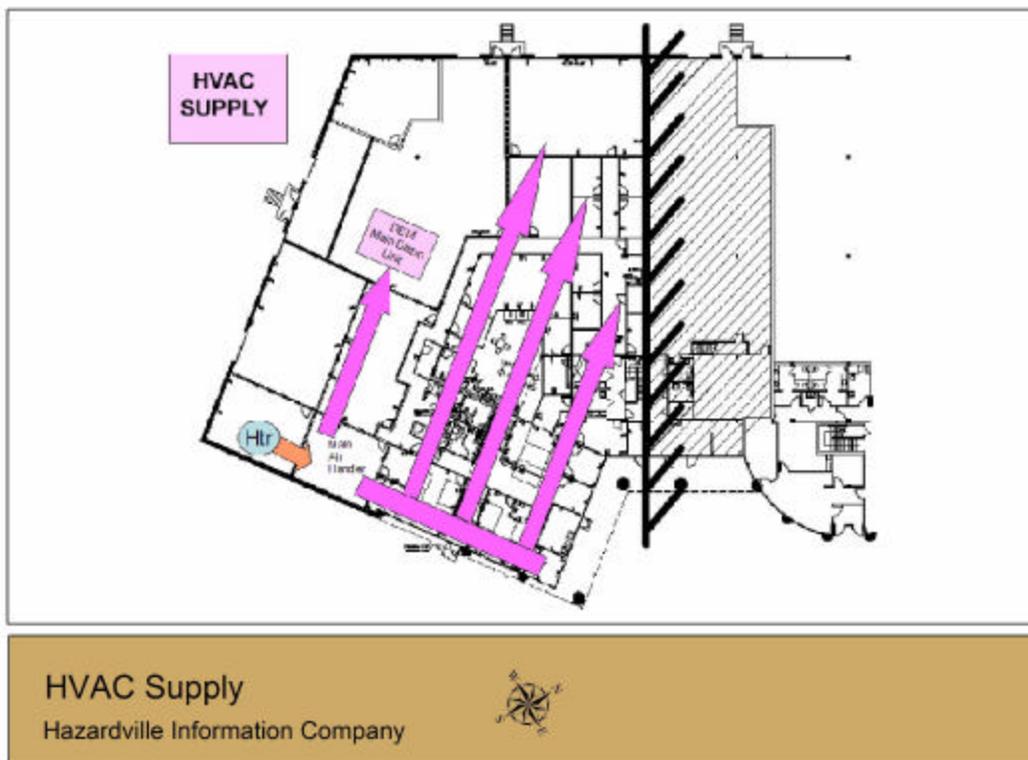
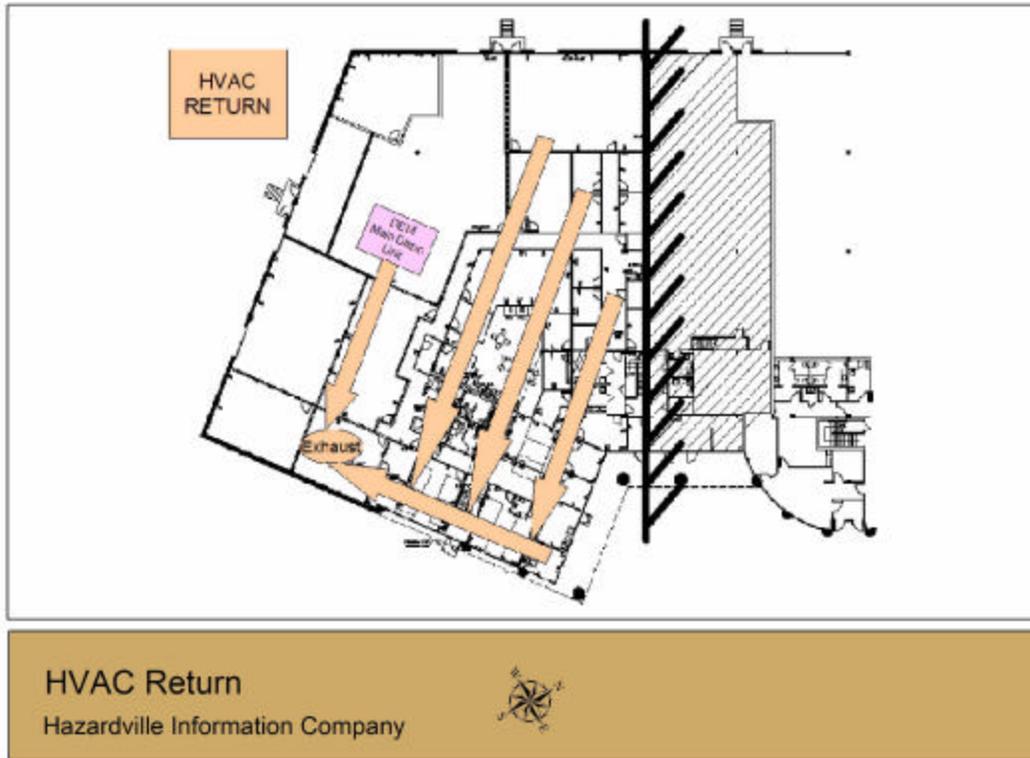


Figure 11. HVAC Supply

The return air for the main office space has sufficient room inside the ductwork and mechanical room area to incorporate additional filters and equipment.



**Figure 12. HVAC Return**

Cooling (or heat removal) is done by two chillers in the M&E room. Three Trane 100-ton chillers are available; normally only two are needed to cover all heat loads. The chillers remove heat from the chilled water system, and use the condenser water system to send the waste heat to two rooftop cooling towers. The chilled water is then routed from the chillers to air handlers for the majority of the building; cooling for the Computer Center and the Communications Center is done by directing chilled water to the DEMs. Chiller operation along with chilled water and condenser water flow are managed from a single control unit in the M&E room. A single chilled water pump provides adequate flow for all cooling situations; a backup pump is available at the push of a button. The same is true for the condenser water pumps.

The air intake is exposed and of typical louver construction.



Figure 13. Air Intake

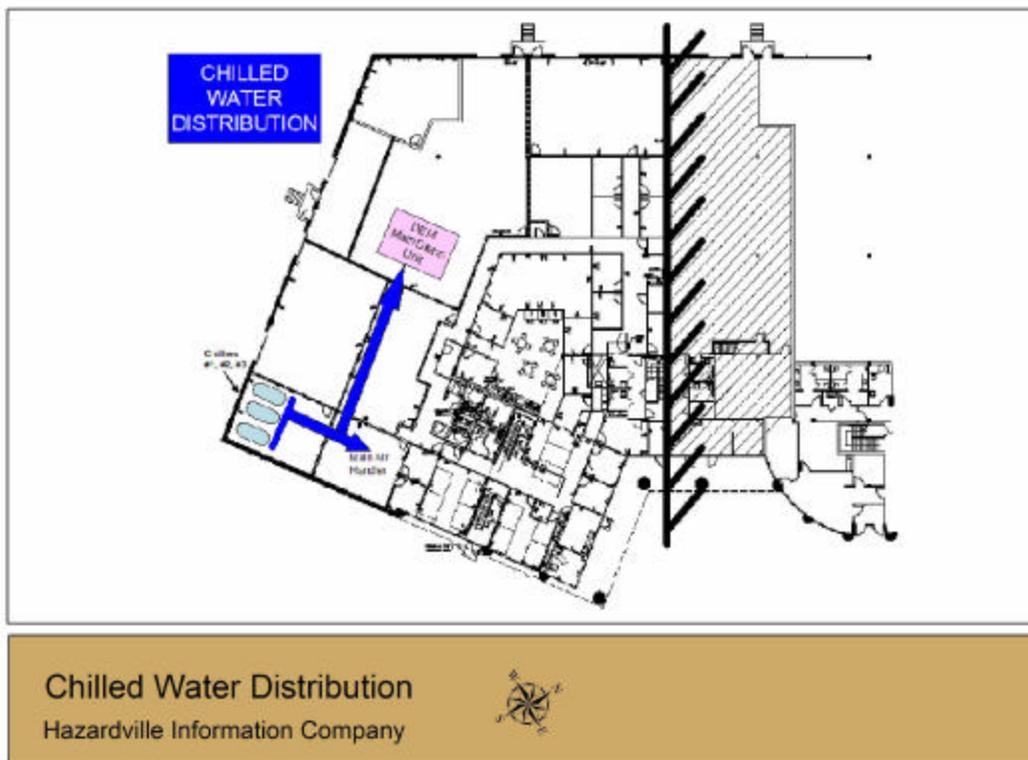


Figure 14. Chilled Water System

The DEMs in the Computer Center and the Communications Center use airflow to transfer heat from electronic equipment to the chilled water, and return cool air to the equipment. Humidity is raised or lowered as necessary for each area of the room. The DEMs operate without the need for frequent monitoring by technicians; parameters and flowrates are controlled from a central station based on the needs of individual pieces of equipment.

Appendix A: Case Study

---

Natural gas enters the building through two meters under the loading dock staircase and goes through the overhead to the M&E room at the building's southwest corner. Branches split off for two gas powered space heaters in the high-bay area by the loading dock. The main gas line goes to the main heater in the M&E room.



Figure 15. Loading Dock Area



Figure 16. Gas Meters Under Stairs

The chillers, pumps, cooling towers, fans, etc., are all powered from the Support Bus (SB). The DEMs and all of the building thermostats receive power from the Computer Center Bus (CCB).

### Fire Protection and Life Safety

A key concern for HIC is fire. The building has been designed to meet the latest National Fire Prevention and Life Safety Codes. Sprinklers are located throughout the building, along with hand-held portable fire extinguishers. There are six exits that can be used for evacuation.

The fire protection and life safety systems consist of a “wet-pipe” single stage sprinkler system throughout the building, ceiling mounted automatic fire and smoke detectors connected to the central business park fire enunciator panel located in the next building and HVAC fire and smoke dampers in the M&E room air handling unit (AHU). There are no manual fire pulls, and the sprinkler system header is continuously pressurized, with water being held back by the temperature actuated valve on the sprinkler head. Each sprinkler head is individually activated by heat; any valve reaching 130° F would open. This system would allow a kitchen or office space fire to be extinguished, without unnecessarily dousing critical computer equipment with water. However, the sprinkler heads are exposed in the overhead of each room, and can be accidentally activated if bumped by a ladder, pole, etc. None of the ingress or egress doors have the new generation illuminating markings, only the standard door or ceiling mounted exit signs and emergency lighting. Should a fire occur, other than the fire detector flashing lights, there is not a mass notification system.



**Figure 17. Sprinkler Head**

There are 20 hand-held dry chemical fire extinguishers located throughout the building, 5 on the mezzanine level, and 15 on the first floor. Filled with monoammonium phosphate under approximately 200-250 pounds pressure, these extinguishers are designed to combat Class A, B and C fires. The fire extinguishers are visually inspected to make sure pressure is in the allowable band on a monthly basis by a local company.

The Computer Center and the Communications Center are equipped like the rest of the building. HIC has a long-term plan to install a clean agent extinguishing system in the electronic spaces, but construction has not started.

The Security Officer maintains the fire evacuation and response plan, has posted fire evacuation routes in key office hallways and break areas, and has a key to the building that has the main fire panel. The main fire panel is located in the lobby area, which is open to unrestricted access during normal business hours. In the event of a fire, the panel alerts the local fire department and the security company.

### **ELECTRICAL SYSTEMS**

Main power for the HIC office is provided by Hazardville Electric Power Company through two transformers outside the building. Two sets of buried transmission lines deliver 12,470 volt (12.47KV) power to the building from a nearby substation.

The two 12.47KV feeders lead to two separate transformers outside the building, one near the north side, and the other near the south side. The two “mini-mite” pad-mounted transformers are rated at 2500KVA, and they reduce the 12.47KV power to 480/277 volts for distribution around the building.

Appendix A: Case Study

---



**Figure 18. One of Two Transformers**

Both transformers are continuously on line, and feed separate loads. Neither is loaded above 50 percent, and a tie breaker allows either transformer to support all building loads, except during the peak cooling months when three chillers are operating.

Backup power for HIC is provided by a single diesel generator, located in a shed in the rear parking lot. Specs for this Detroit Diesel Model 1250DS-4 Spectrum unit follow:

<b>Model 12V4000 Engine</b>	<b>Model 7M4052 Generator</b>
4-Cycle	Voltage 480/277 VAC
Turbocharged, Intercooled	3 Phase/60 Hz
V-12 Cylinder Configuration	1250KW/1563KVA
2975 Cubic Inch Displacement	1879 Amps
1800 RPM	Sustained Short Circuit Current up to
Max Power 1380 KW/1850 BHP	300 Percent of Rated for 10 Seconds
Exhaust Temperature 402° C/755° F	Brushless, Rotating-Field
Water Cooled, Electric Start	Pilot Excited
319 GPH Fuel Flow at 100 Percent Load	
240 GPH Fuel Flow at 75 Percent Load	1 Year Limited Warranty
165 GPH Fuel Flow at 50 Percent Load	

The backup generator is equipped with a 50-gallon day tank, normally kept at least 80 percent full. The day tank draws fuel from a 2,000-gallon main fuel tank, buried under the parking lot near the diesel generator shed. A small electric pump is used to fill the day tank when necessary.

The day tank's level is measured using a sightglass. The level of the main fuel tank is measured with a probe each quarter by a visiting Detroit Diesel representative, who also starts the engine to run unloaded for about 20 minutes. Fuel is delivered by a local contractor, who normally responds the day after being called.

**Appendix A: Case Study**

---

The diesel generator is configured to automatically start upon loss of commercial power to the CCB. This happens about twice a year due to electrical storms or utility maintenance in the neighborhood. An automatic bus transfer switch aligns the generator to the CCB as soon as the generator is ready to support the bus loads. This normally takes less than 5 seconds. In addition, a manually operated tie breaker is available to supply backup power to the SB via the CCB; however, the SB cannot receive backup power by itself. The backup diesel generator has never had to support HIC's power demands for longer than about 2 hours, and never with more than one chiller operating. It has never been tested for an extended period under heavy load.

An uninterruptible power supply (UPS) is located inside the building's "high-bay" area. Rated at 1000KVA, it is designed to support all loads on the CCB for up to 60 minutes. The diesel generator has never taken more than 30 seconds to start and assume the bus loads. If the diesel generator did not start on a loss of commercial power, 60 minutes would be ample time for HIC personnel to conduct an orderly shutdown of Computer Center equipment.

The batteries to support the UPS are in a small room next to the UPS room. The only instrumentation in the room is a thermometer. The 50 lead-acid batteries are inspected semi-annually by the manufacturer's representative. A capacity test discharge was conducted when the batteries were installed 2 years ago. The 60-minute endurance was calculated from that test.

HIC's electrical loads are divided between two main electrical buses, the CCB and the SB. They are located in separate "closets" of the building. A tie breaker allows the buses to be connected, so they can be powered by a single main transformer, or to allow SB loads to be carried by the backup diesel generator. The system is monitored by a digital energy management system, which provides indications, alarms, and instructions.

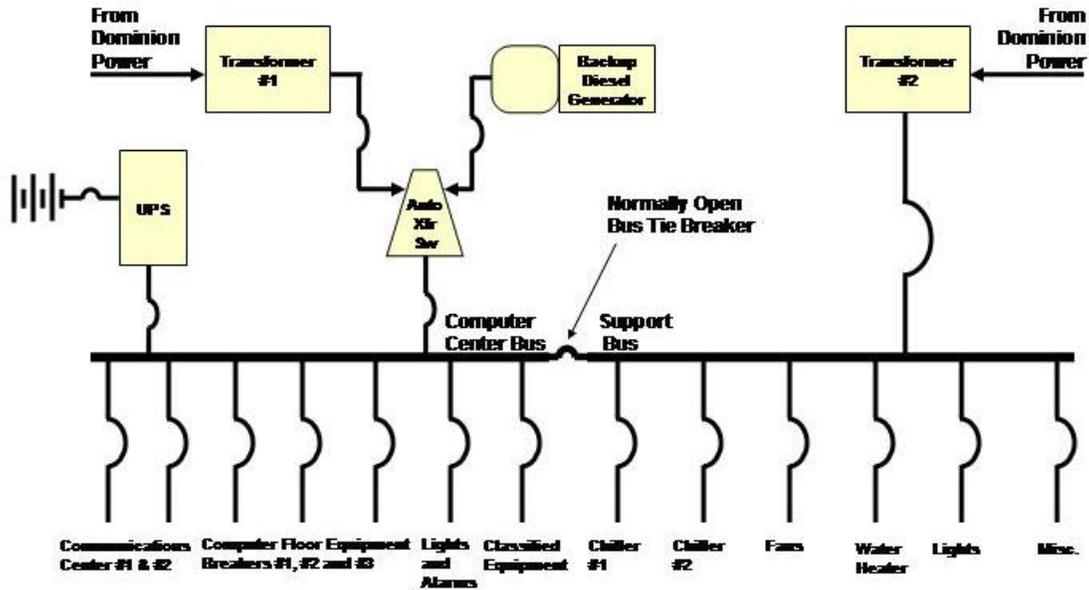


Figure 19. Electrical “One-Line” Diagram

Typical of many commercial office buildings, the mechanical and electrical systems share common utility penetrations and floor space. There are no redundant utility feeds to the building from different directions.

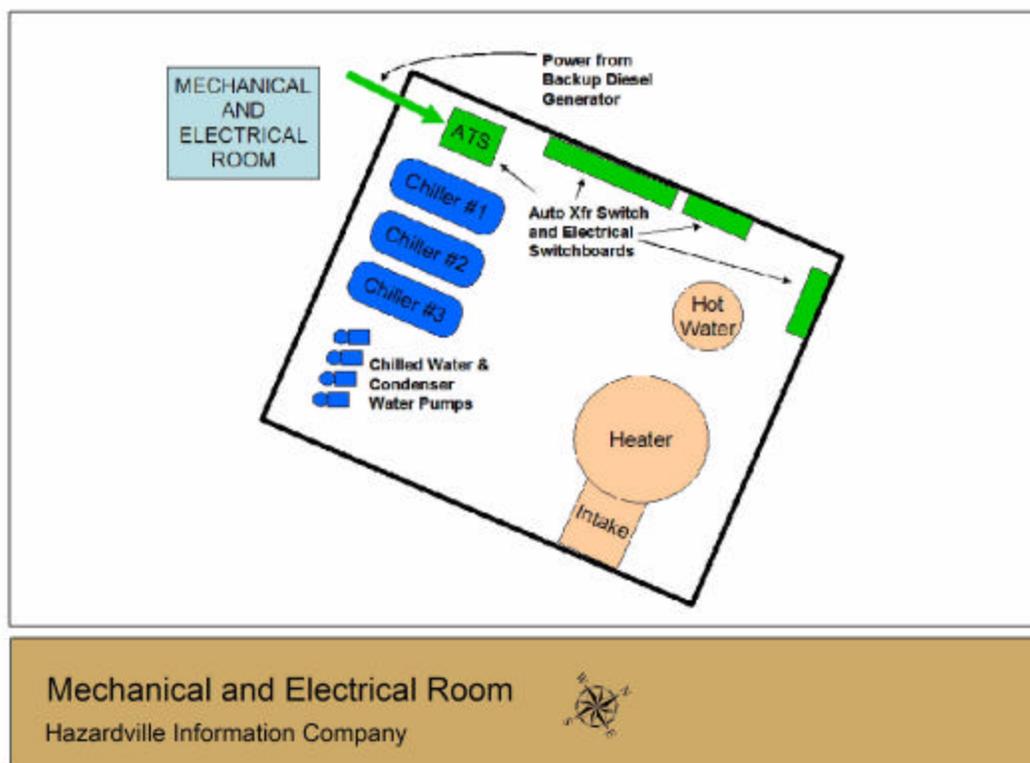


Figure 20. Mechanical and Electrical Room

## INFORMATION OPERATIONS

The Computer Center is the heart of HIC's operations. The rest of HIC exists to support the Computer Center.

### Hardware

The Computer Center is composed of several interconnected systems and one independent system for classified data processing. The systems run VMS, Unix, or Windows. Although the equipment list changes almost monthly as systems are upgraded and new clients' needs are being met, as of April 2003, the computers included the following:

- One 4-processor Silicon Graphics Power Challenge
- Three dual-processor Silicon Graphics Origin 200 servers
- One dual-processor Silicon Graphics Octane
- Five Microway Dec Alpha 500 MHz systems (four Unix, one VMS)
- Three DEC Alpha 600 5/266 systems
- Two IBM RISC 6000/560 systems with 160 and 128 Megabytes (MB) of memory
- One Stardent 3000 with 128 MB of memory, triple scalar & vector processors

Appendix A: Case Study

---

- One DEC Alpha-based (RISC) Model 3000/400 VMS workstation
- One DEC Vaxstation 4000/90 system with 128 MB of memory
- Sixteen Windows based workstations



**Figure 21. Computer Center**

All computers have access to large-capacity disk storage units, with shared mounting of major disk units throughout the complex. The VMS systems are configured as a Vax cluster; the Unix systems have common user accounts and files. The major systems are reachable from throughout the center and also through an Ethernet. The networks interface to the company-wide network and through it to the Internet.

Because some customers rely on HIC to support their data storage needs, the Computer Center also contains a massive data storage “jukebox.” A StoreAll Model 5500 provides fully automated storage, using robot arms to provide rapid retrieval. Its capabilities include:

- 3.0 Terabyte Total Capacity
- 2.5 Megabyte Per Second (MBps) Transfer Rate
- 500 CD Per Hour Change Rate
- 10,000 CD Storage Rack

Client data is backed up as requested by the clients, as frequently as once per day. The Back-O-Matic digital backup system manages the backup process, selecting which data are backed up on which day. All backups are done to CD; these are stored in the StoreAll Model 5500. HIC maintains an off-site storage location for clients that require backup data to be stored at a separate site. Classified backup data for certain government clients are stored in a special fireproof safe in the Secure Space.

Backup procedures for HIC’s computer operating systems, digital telephones and other company systems are similar as for their clients. Most of HIC’s computer systems can be used to backup another system. For those systems without in-house backups, replacement sources are identified. In most cases, replacement hardware can be delivered and setup within 2 days.

## COMMUNICATIONS

### Data

HIC has two T1 lines and one T3 line connected at the demark to ATT's high performance backbone network. The ATT fiber connectivity provides more than enough bandwidth for HIC's current needs and planned future expansion.

### Telecom and Network Connections

- Two T1 lines (1.544 MBps)
- One T3 (45 MBps)
- Frame Relay
- Narrowband ISDN (64/128 KBps)



Figure 22. Telecom and Network Connections



Figure 23. Telecom and Network Connections

**Appendix A: Case Study**

---

The Cisco powered network features multiple 7500 VXR+ routers. Border Gateway Protocol (BGP) reroutes traffic between the routers and to the Internet. A variety of switches in the Communications Center and at client sites are used to ensure connectivity. Some clients use Hot Standby Routing Protocol (HSRP), which provides additional redundancy.

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.

Communications to support HIC's classified government clients cannot be discussed in detail. Nevertheless, they used leased lines for point-to-point connectivity, and they are robust, with diversity and redundancy built in.

**Voice**

Although HIC does not provide voice communications services to customers, the need to communicate with them quickly and reliably is important. Therefore, the company has invested in NEC DS2000 telephone systems, which come with 8-slot cabinets that can handle 32 lines from 48 stations. The system's digital processor provides reliability, speed, and features to keep HIC staff members in touch with their customers.

**PHYSICAL SECURITY**

Much of the company's guidance for security comes from the National Industrial Security Program Operating Manual (NISPOM), the government's guide to protecting contractor facilities. The NISPOM is promulgated by the Defense Security Service (DSS) and is available on the World Wide Web at: [http://www.dss.mil/isec/nispom\\_0195.htm](http://www.dss.mil/isec/nispom_0195.htm).

HIC's Security Officer uses a layered approach to physical security. The outermost physical security layer is provided by a contract security firm and the Defense Protective Service (DPS).

The contract security firm periodically patrols the parking lots in marked vehicles. The security officers are not armed, but they carry cellular phones to contact the local police. These officers do not have security clearances, and are not allowed to enter the HIC Headquarters if no employees are present.

The DPS officers patrol the entire National Capital Region (NCR) and are tasked to respond to emergencies at Defense Department or contractor facilities. DPS officers are armed and have law enforcement authority. They are allowed to enter the HIC building, but normally do not as part of their rounds.

The parking lot behind the HIC office is well lit and monitored by older generation analog CCTV cameras using telephone wires that are connected to video displays in the HIC Security Officer's office and recorded on standard VHS tape. The CCTVs are commercial grade black

Appendix A: Case Study

---

and white with a 180-degree field of view that the security officer can control via the display panel. The front parking lot is lit, but not monitored.

HIC's middle layer of security is the building envelope. The building is monitored by door and window alarms, which connect to ADT, the nationwide alarm company. Unauthorized opening of any door or window will immediately notify ADT via telephone. ADT will normally call the HIC Security Office prior to contacting the police and DPS. HIC employees have proximity cards to allow them to enter the front and loading dock doors without activating the alarm.



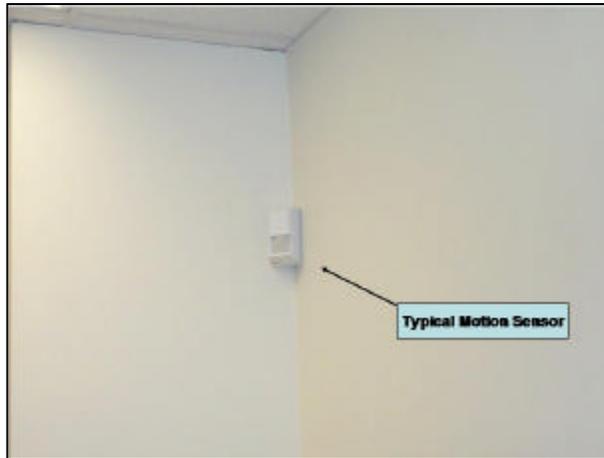
Figure 24. Proximity Cards Readers and Alarms



Figure 25. Security Lighting



**Figure 26. Electronic Badge Reader**



**Figure 27. Motion Detector**

The innermost layer of physical security involves the Computer Center and the Communications Center. Equipped with locked doors, these two rooms meet the government's requirements for handling classified material. Only authorized employees possess the necessary proximity cards and PINs to gain access. Unauthorized access to either space will sound sirens, flash lights, and notify the HIC Security Officer and DPS. The access doors are not manned or monitored with cameras. The crawl spaces created by the raised floor in the Computer Center are barricaded by a wire fence in the three locations where it can be accessed from other parts of the building.

## EMERGENCY RESPONSE

In the event of an emergency, HIC senior management use the large conference room as an Emergency Operations Center. The room is equipped with network and telephone connections and cell phones are able to receive a signal.



**Figure 28. Large Conference Room, Emergency Operations**

The nearest fire station is approximately 2½ miles north of the HIC Headquarters. Seven other fire stations are within 5 miles of the site. Firefighters are trained as Emergency Medical Technicians (EMTs) and Hazardous Material Technicians. Many are also skilled in technical rescue (high places, confined spaces, etc.). Ambulances are also dispatched from these stations. Emergency response time for emergencies is estimated to be 8-10 minutes. Fire hydrants are available in the office park.

The nearest hospital with an emergency room is 5 miles away. Other emergency response information includes:

- Exit signs: Located above each exit.
- Battery operated emergency lights: Strategically placed throughout the building.
- Emergency exits: Normally closed and locked doors have “panic bars” for use in emergencies.
- Announcing system: The telephone system has a building-wide announcing feature that can be activated by pressing one button at any phone.
- Evacuation plan and escape ladders for the mezzanine: None.
- Emergency stairway: Located far from main stairs.

## NATURAL AND TECHNOLOGICAL HAZARDS

### Natural Disasters Hazards

The county's Local Emergency Planning Committee provided the following information regarding natural disasters:

- The state experiences an average of 7 tornadoes/hurricanes per year.
- The area's earthquake risk is 1 (Scale 0-4).
- The state experiences 80-100 days per year with one or more lightning strikes.

### Technological Disasters Hazards

HIC is surrounded by a number of commercial activities and key national critical infrastructure to include HAZMAT facilities, HAZMAT being transported on the roads and rails, a nearby fuel tank farm, and an airport.

#### Hazardous Material (HAZMAT) Facilities

There are two large manufacturing plants with large quantities of hazardous materials stored on site within 2 miles of the HIC Headquarters, one to the north and the other to the southwest. In addition, there are more than a dozen Tier II HAZMAT Facilities within 3 miles of the building (in all directions).

The prevailing weather pattern for the area in the summer and fall is from the south Atlantic and the Gulf of Mexico. Warm, moist air brings thunderstorms and higher humidity. In the fall, cooler air from the north and west returns. Winter weather blasts across the state from the northern or central part of the continent. With no other weather activity, the prevailing wind is normally from the south in the Summer and from the north-northwest in the Winter.

None of the nearby facilities were contacted during this analysis. There is no information available regarding accidents or incidents involving these facilities.

#### Highway Movement of Hazardous Material (HAZMAT)

A major interstate highway is located within ¼ mile of the HIC Headquarters. Approximately 5,000 trucks per day pass the HIC office on the nearby interstate highway. About 30 percent of these trucks (1,500 trucks/day) carry placards indicating that HAZMAT is aboard, but only about 5 percent (250 trucks/day) carry sufficient HAZMAT to warrant placarding.

Approximately 50 percent of the HAZMAT passing the HIC office is Class 3 (flammable and combustible liquids). Class 2 (gases) and Class 8 (corrosives) each constitute about 15 percent. Approximately 10 percent of the trucks carry more than one class of HAZMAT.



**Figure 29. HAZMAT Truck on Interstate Highway**

The State Police Department inspects 5-10 percent of the HAZMAT carrying trucks on interstate highways.

Approximately 476 incidents involving the transportation of HAZMAT occur each year in the county in which HIC is located. Most of these involve flammable gas and liquids. Only one HAZMAT incident took place on a highway within 2 miles of HIC in the period 1995 to 2002.

#### Rail Movement of Hazardous Material

CSX Transportation and Norfolk-Southern Railway maintain a transportation corridor approximately ½ mile from HIC. There appear to be no restrictions on the material carried along these rail lines. Neither company was available for interviews.

Nevertheless, rail traffic has been informally monitored in this area. It is estimated that approximately 10,000 railcars of HAZMAT move through this area each year. Hazardous materials range from liquid petroleum products to chlorine to anhydrous ammonia.

There are no recent records of any HAZMAT spills or incidents involving rail transportation in the county in which HIC is located.

#### Liquid Fuels

A leg of the Piedmont Petroleum Pipeline (PPP) runs underneath the office park in the vicinity of HIC Headquarters. Part of Piedmont's regional network, this portion of the pipeline normally carries a variety of refined products, including commercial and military jet fuels, diesel and three grades of gasoline, home heating fuels, etc. Four buried pipes carry approximately 20 million gallons per day.

**Appendix A: Case Study**

---

There is no available information regarding any pipeline ruptures or incidents in the vicinity of HIC.

Connected to the pipeline, less than 1 mile from HIC, is a 20-million gallon capacity fuel farm. Operated by the Shellexxico Company, this tank farm stores a variety of petroleum products, primarily gasoline. Although representatives of Shellexxico were unavailable for an interview, their operations appear to conform to industry standards. Thirteen tank trucks were observed leaving the tank farm in a 1- hour period, indicating a calculated movement rate of approximately 300 trucks per day (about 3 million gallons of fuel).



**Figure 30. Shellexxico Tank Farm**

Based on terrain elevation data, the ground level of the tank farm is 6 feet higher than the ground level at HIC. Only some of the fuel tanks are bermed, but leaking fuel is not likely to reach HIC's office park; the interstate highway between the two is 10 feet lower than the tank farm.

Air Traffic

Two airports are in the vicinity of HIC. One is a major international airport approximately 8 miles away. The other is a small, but busy general aviation airport less than 2 miles away. The office park in which HIC is located is in direct line with one of the approach and departure paths of this regional airport.

The website for the regional airport indicates it is capable of handling business jets, providing jet fuel and high octane aviation gasoline and other services.

The airport is tower controlled and handles approximately 100,000 flights per year.

## **THREAT ANALYSIS**

The following information was obtained from the regional office of the FBI and the State Police:

### **Terrorist Threat**

Since September 11, 2001, the terrorist threat in the area has been Yellow or Orange. Yellow has been the norm, except for the anniversary of the 9/11 attacks and during the recent war in Iraq.

**Yellow Definition:** Elevated risk of terrorist attack, but a specific region of the United States or target has not been identified

**Orange Definition:** Credible intelligence indicates that there is a high risk of a local terrorist attack, but a specific target has not been identified.

The elevated and high threat condition is not due to any specific information or threat to the area in which the HIC office is located, but rather due to the proximity to the metropolitan area, nearby military installations, etc.

There is no known threat to HIC Incorporated, any of its officers or employees. There are no known threats to any of the companies within the office park. Nearby commercial entities that are likely terrorist targets include the Shellexico tank farm, two rail lines, the busy interstate highway, and the transformer substation.

Although HIC is probably not a primary target, there is a military installation within 10 miles, two large prime contractors and one federal agency office in the business park, and potential collateral damage or targeting of HIC as an alternate if those organizations are targeted and attacked.

### **Intelligence Threat**

The HIC Security Officer maintains close coordination with government security officers and law enforcement agents as part of his normal duties. All HIC employees hold security clearances, Secret or higher. This makes them targets for foreign intelligence services. Although there has been no known case of an HIC employee being approached by a foreign intelligence agent, this is certainly a possibility. The company follows counterintelligence guidance and procedures from the Defense Security Service (DSS) and the Defense Intelligence Agency (DIA) regarding:

- Risk management of classified programs in industry
- Threat awareness
- Deterrence of illegal technology transfers
- Facilitating the prevention of economic espionage in defense contractor facilities

Appendix A: Case Study

---

## Criminal Threat

### Gangs and Drugs

There are several gangs operating in the metropolitan area and they have been responsible for a number of gang related murders. Drug activity continues to be a problem in the metropolitan area, but less so in the suburbs. There has not been any gang or drug activity near the HIC building.

### Violent Crime

The 2002 Crime Index, which is composed of murder, forcible rape, robbery, aggravated assault, burglary, larceny-theft, and motor vehicle theft, was relatively unchanged from 2001 figures. In 2002, a woman waiting at a bus stop near HIC's office complex was assaulted; there have been no other reported crimes in the "neighborhood."

### **Year 2000 Area Crime Comparison (Rates per 100,000 population)**

<u>Crime</u>	<u>County</u>	<u>State</u>	<u>United States</u>
Murder	1.30	5.7	5.5
Rape	10.74	22.8	32.0
Robbery	41.32	88.9	144.9
Aggravated Assault	40.02	164.3	323.6
Burglary	155.95	429.9	728.4
Larceny	1950.84	2064.8	2457.3
Vehicle Theft	197.27	251.6	414.2

Other Crimes: Employee Fraud and Identity Theft have become a growing problem in the state in which HIC is located. County crime statistics indicate these problems are prevalent nearby, and a nearby business lost \$11,000 to "trusted employees" in 2001, but there have been no indications of such problems at HIC.

## **DESIGN BASIS THREAT**

The senior management of HIC reviewed the site, building, and threat information collected, and determined the Design Basis Threat to be:

Appendix A: Case Study

---

**Explosive Blast:** Car Bomb - approximately 250 lb. TNT equivalent. Truck Bomb - approximately 5,000 lb. TNT equivalent (Murrah Federal Building class weapon)

**Chemical:** Large quantity gasoline spill and toxic plume from the adjacent tank farm, small quantity (tanker truck and rail car size) spills of HAZMAT materials (chlorine).

**Biological:** Anthrax delivered by mail or in packages, smallpox distributed by spray mechanism mounted on truck or aircraft around metropolitan area.

**Radiological:** Small “dirty” bomb detonation within the 10-mile radius of the HIC building.

**Criminal Activity/Armed Attack:** High powered rifle or handgun exterior shooting (sniper attack or direct assault on key staff, damage to infrastructure [i.e., transformers, chillers, etc.]).

**Cyber Attack:** Focus on IT and building systems infrastructure (SCADA, alarms, etc.) accessible via internet access. Computer Data Center and Communications Center supporting infrastructure (e.g., firewalls, routers, main distribution rooms, backup tapes storage, etc.) location, redundancy, and power supply meet NIST and industry standards for physical access and protection. The analysis is not to include information assurance assessment activities (e.g., password, network monitoring, host and intrusion detection, etc.).

## LEVEL OF PROTECTION

Based on the Design Basis Threat and after reviewing the General Services Administration (GSA) and Department of Defense (DoD) standards, senior management selected preliminary Levels of Protection most applicable to HIC, with the guidance that adoption of any recommendations would be to the most stringent standard and would be in compliance with life safety codes. After the vulnerability and risk assessments were complete and mitigation options developed, final selection of mitigation options would be made by senior management and determined on a benefit-cost and risk reduction basis. The Levels of Protection to be used as the basis for the vulnerability and risk assessments are:

### GSA Level II

A Level II facility has between 11 and 150 employees and from 2,500 to 80,000 square feet.

#### 1. Perimeter Security

a. Security control for parking (surface lots, adjacent structures, underground garages under the Lessor's control) is solely limited to the assignment (marked "reserved") of authorized Government parking spaces and vehicles.

b. Adequate lighting, with emergency power backup, for the exterior of the building is required. Parking areas shall also be adequately lighted.

Appendix A: Case Study

---

- c. 24-hour CCTV surveillance cameras with time-lapse video recording **may** be required as deemed necessary by a Security Specialist.
- d. Application of shatter-resistant material shall be applied on exterior windows.

2. Entry Security

- a. Security Guards **may** be required, as deemed necessary by a Security Specialist.
- b. Intrusion Detection System (IDS) with central monitoring capability **may** be required, as deemed necessary by a Security Specialist, for the building exterior.
- c. Peepholes in exterior doors **may** be required, as deemed necessary by a Security Specialist, when an IDS is not appropriate.
- d. An intercom system, used in conjunction with a peephole, **may** be required as deemed necessary by a Security Specialist.
- e. Entry control with CCTV and door strikes **may** be required to allow employees to view and communicate remotely with visitors before allowing access, as deemed necessary by a Security Specialist.
- f. Exterior entrances shall have high security locks.

3. Interior Security

- a. A visitor control/screening system is not required for these levels.
- b. Utility areas shall be secured and only authorized personnel shall have access.
- c. Emergency power sources to critical systems (i.e., alarm systems, radio communications, computer facilities, CCTV monitoring, fire detection, entry control devices, etc.) are required.
- d. The following requirements pertain to the added protection of the building environment from airborne chemical, biological, or radiological attacks.
  - (1) Access to mechanical areas and building roofs shall be strictly controlled.
  - (2) Access to building information, including mechanical, electrical, vertical transport, fire and life safety, security system plans and schematics, computer automation systems, and emergency operations procedures shall be required. Such information shall be released to

Appendix A: Case Study

---

authorized personnel only. Names and locations of Government tenants shall not be disclosed within any publicly accessed document or record.

(3) Procedures (should airborne hazards be suspected or found) are required for the notification of the lessor's building manager, building security guard desk, local emergency personnel, or other Government emergency personnel, for the possible shutdown of air handling units serving any possibly affected areas.

4. Administrative Procedures

a. Building managers and owners are required to cooperate with and participate in the development and implementation of Government Occupant Emergency Plans (OEPs).

b. Conduct background security checks and/or establish security control procedures for contract service personnel as deemed necessary.

c. The Government reserves the right, at its own expense and manpower, to temporarily upgrade security during heightened security conditions due to emergency situations such as terrorist attacks, natural disaster and civil unrest. The measures shall be in accordance with the latest version of the Homeland Security Advisory System.

5. Blast/Setback Standards

a. The following blast/setback standards shall be met:

1. For Level II, a 20 foot setback<sup>1</sup> guideline with appropriate window glazing, as prescribed by WINGARD 3.15 or later or WINLAC 4.3 software, to achieve a glazing performance condition of 3b<sup>2</sup> and a façade protection level of "medium"<sup>3</sup> given a blast load standard of 4 psi/28 psi-msec is required.

<sup>1</sup> Setback refers to the distance from the face of the building's exterior to the protected/defended perimeter (i.e., any potential point of explosion). This would mean the distance from the building to the curb or other boundary protected by bollards, planters, or other street furniture. Such potential points of explosion may be, but not limited to, such areas that could be accessible by any motorized vehicle (i.e., street, alley, sidewalk, driveway, parking lot).

<sup>2</sup> Glazing Performance Condition 3b provides for a high protection level and a low hazard level. For a blast of 4psi/28psi-msec, the glazing cracks and fragments enter the space and land on the floor not further than 10 feet from the window.

<sup>3</sup> A "Medium Level Protection" to the facade will result in moderate, but repairable damage. The facility or protected space will sustain a significant degree of damage, but the structure should be reusable. Some casualties may occur and assets may be damaged. Building elements other than major structural members may require replacement.

Appendix A: Case Study

---

**DoD Standards**

HIC senior management evaluated the DoD standards and determined that they would attempt to meet the intent and objective of as many of the recommendations as possible. Of particular concern are blast, CBR, and associated operations/locations of functions and equipment such as mailrooms, dumpsters, loading docks, and emergency shut down.

The DoD level of protection selected is “low”, and the building category is “Inhabited Building”.

<b>UFC 4-010-01 APPENDIX B</b>	
<b>DoD MINIMUM ANTITERRORISM STANDARDS FOR NEW AND EXISTING BUILDINGS</b>	
Standard 1	Minimum Standoff Distances
Standard 2	Unobstructed Space
Standard 3	Drive-Up/Drop-Off Areas
Standard 4	Access Roads
Standard 5	Parking Beneath Buildings or on Rooftops
Standard 6	Progressive Collapse Avoidance
Standard 7	Structural Isolation
Standard 8	Building Overhangs
Standard 9	Exterior Masonry Walls
Standard 10	Windows and Glazed Doors
Standard 11	Building Entrance Layout
Standard 12	Exterior Doors
Standard 13	Mailrooms
Standard 14	Roof Access

Appendix A: Case Study

---

Standard 15	Overhead Mounted Architectural Features
Standard 16	Air Intakes
Standard 17	Mailroom Ventilation
Standard 18	Emergency Air Distribution Shutoff
Standard 19	Utility Distribution and Installation
Standard 20	Equipment Bracing
Standard 21	Under Building Access
Standard 22	Mass Notification
Recommendation 1	Vehicle Access Points
Recommendation 2	High-Speed Vehicle Approaches
Recommendation 3	Vantage Points
Recommendation 4	Drive-Up/Drop-Off
Recommendation 5	Building Location
Recommendation 6	Railroad Location
Recommendation 7	Access Control for Family Housing
Recommendation 8	Standoff for Family Housing
Recommendation 9	Minimize Secondary Debris
Recommendation 10	Structural Redundancy
Recommendation 11	Internal Circulation
Recommendation 12	Visitor Control
Recommendation 13	Asset Location
Recommendation 14	Room Layout
Recommendation 15	External Hallways
Recommendation 16	Windows

---

Appendix A: Case Study

<b>Level of Protection</b>	<b>Potential Structural Damage</b>	<b>Potential Door and Glazing Hazards</b>	<b>Potential Injury</b>
<b>Low</b>	Damaged – unrepairable. Major deformation of nonstructural elements and secondary structural members and minor deformation of primary structural members, but progressive collapse is unlikely.	Glazing will break, but fall within 1 meter of the wall or otherwise not present a significant fragment hazard. Doors may fail, but they will rebound out of their frames, presenting minimal hazards.	Majority of personnel suffer significant injuries. There may be a few (<10%) fatalities

<b>Location</b>	<b>Building Category</b>	<b>Standoff Distance or Separation Requirements</b>			
		<b>Applicable Level of Protection</b>	<b>Conventional Construction Stand-off Distance</b>	<b>Effective Stand-off Distance</b>	<b>Applicable Explosives Weight</b>
Controlled Perimeter or Parking and Roadways without a Controlled Perimeter	Inhabited Building	Very Low	25 M 82 ft	10 M 33 ft	Approx 250 lbs

## DoD Stand-off Distance

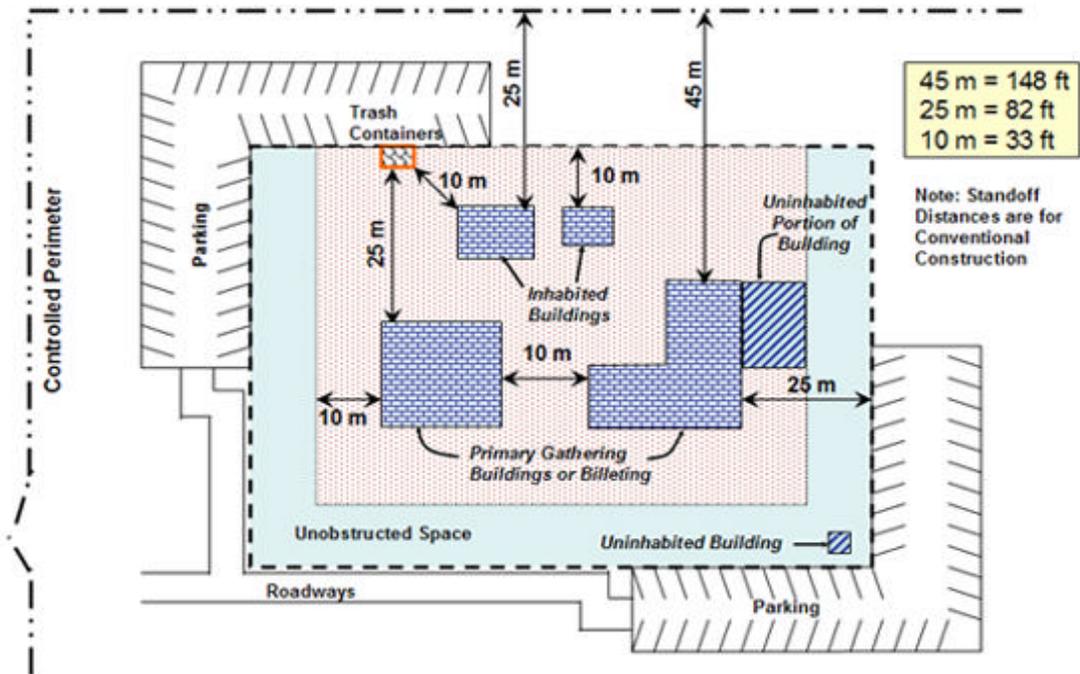


Figure 31. DoD Stand-off Distance