

## Unit V

---

|                     |                                       |             |            |
|---------------------|---------------------------------------|-------------|------------|
| <b>COURSE TITLE</b> | Building Design for Homeland Security | <b>TIME</b> | 45 minutes |
|---------------------|---------------------------------------|-------------|------------|

---

|                   |                                   |
|-------------------|-----------------------------------|
| <b>UNIT TITLE</b> | Risk Assessment / Risk Management |
|-------------------|-----------------------------------|

---

|                   |   |
|-------------------|---|
| <b>OBJECTIVES</b> | <ol style="list-style-type: none"><li>1. Explain what constitutes risk</li><li>2. Evaluate risk using the Threat-Vulnerability (Risk) Matrix to capture assessment information</li><li>3. Provide a numerical rating for risk and justify the basis for the rating</li><li>4. Identify top risks for asset-threat/hazard pairs of interest that should receive measures to mitigate vulnerabilities and reduce risk</li></ol> |
|-------------------|---|

---

|              |  |
|--------------|--|
| <b>SCOPE</b> | <p>The following topics will be covered in this unit:</p> <ol style="list-style-type: none"><li>1. Definition of risk and the various components to determine a risk rating.</li><li>2. The FEMA 426 approach to determining risk.</li><li>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.</li><li>4. The relationships between high risk, the need for mitigation measures, and the need to identify a Design Basis Threat and Level of Protection.</li><li>5. Activity: Determine the risk rating for the asset-threat/hazard pairs of interest. Identify the top three risk ratings for the Case Study.</li></ol> |
|--------------|--|

---

|                   |  |
|-------------------|--|
| <b>REFERENCES</b> | <ol style="list-style-type: none"><li>1. FEMA 426, <i>Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings</i>, pages 1-35 to 1-44</li><li>2. FEMA 452, <i>Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings</i>, pages 4-1 to 4-9</li><li>3. Case Study – Appendix A: Suburban, Hazardville Information Company or Appendix B: Urban, HazardCorp Building as selected</li><li>4. Student Manual, Unit V-A or Unit V-B as selected</li><li>5. Unit V visuals</li></ol> |
|-------------------|--|

---

|                     |  |
|---------------------|--|
| <b>REQUIREMENTS</b> | <ol style="list-style-type: none"><li>1. FEMA 426, <i>Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings</i> (one per student)</li><li>2. FEMA 452, <i>Risk Assessment: A How-To Guide to Mitigate</i></li></ol> |
|---------------------|--|

---

*Potential Terrorist Attacks Against Buildings* (one per student)

3. Instructor Guide, Unit V
4. Student Manual (one per student) for selected Case Study
5. Overhead projector or computer display unit
6. Unit V visuals
7. Risk Matrix poster and box of dry-erase markers (one per team)
8. Chart paper, easel, and markers

**UNIT V OUTLINE**

|  | <u>Time</u> | <u>Page</u> |
|--|-------------|-------------|
| V. Risk Assessment / Risk Management   | 45 minutes  | IG V-1      |
| 1. Introduction and Unit Overview  | 5 minutes   | IG V-5      |
| 2. Risk and Rating Approaches  | 7 minutes   | IG V-7      |
| 3. Selecting Mitigation Measures   | 5 minutes   | IG V-10     |
| 4. Process Review/Summary/Transition   | 3 minutes   | IG V-12     |
| 5. Activity: Risk Rating<br>(Version <b>A Suburban</b> )<br>[15 minutes for students, 10 minutes for review] | 25 minutes  | IG V-A-15   |
| 6. Activity: Risk Rating<br>(Version <b>B Urban</b> )<br>[15 minutes for students, 10 minutes for review]    | 25 minutes  | IG V-B-18   |

**PREPARING TO TEACH THIS UNIT**

- **Tailoring Content to the Local Area:** This is a generic instruction unit that does not have any specific capability for linking to the Local Area.

The Instructor will define risk by its components and the approach used in this unit to determine risk. An example will be used to show the students how to determine and evaluate the risk rating for each asset-threat/hazard pair of interest in the threat-vulnerability (risk) matrix. The Instructor will also discuss the relationship between an identified high risk asset-threat/hazard pair of interest and the need for mitigation measures to reduce that risk by reducing the vulnerability rating.

- **Optional Activity:** There are no optional activities in this unit, except Student Activity questions that are applicable to the selected Case Study (Suburban or Urban).
- **Activity:** The student activity is primarily a math exercise in multiplying threat, asset value, and vulnerability ratings to determine the risk rating and then compare it against the risk

rating scale. The top three risks should receive additional emphasis during an actual vulnerability assessment to validate the risk by identifying vulnerabilities and as an input to select mitigation measures.

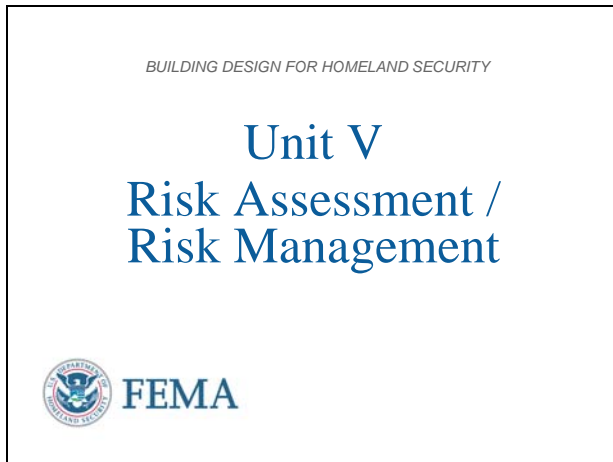
- Refer students to their Student Manuals for worksheets and activities.
- Direct students to the appropriate page in the Student Manual.
- Instruct the students to read the activity instructions found in the Student Manual.
- Explain that the risk ratings determined by the team must be transferred to the Risk Matrix poster.
- Tell students how long they have to work on the requirements.
- While students are working, all instructors should closely observe the groups' process and progress. If any groups are struggling, immediately assist them by clarifying the assignment and providing as much help as is necessary for the groups to complete the requirement in the allotted time. Also, monitor each group for full participation of all members. For example, ask any student who is not fully engaged a question that requires his/her viewpoint to be presented to the group.
- At the end of the working period, reconvene the class.
- After the students have completed the assignment, “walk through” the activity with the students during the plenary session. Call on different teams to provide the answer(s) for each question. Then simply ask if anyone disagrees. If the answer is correct and no one disagrees, state that the answer is correct and move on to the next requirement. If there is disagreement, allow some discussion of rationale, provide the “school solution” and move on.
- If time is short, simply provide the “school solution” and ask for questions. Do not end the activity without ensuring that students know if their answers are correct or at least on the right track.
- Ask for and answer questions.

*This page intentionally left blank*

INSTRUCTOR NOTES

CONTENT/ACTIVITY

VISUAL V-1



**Introduction and Unit Overview**

This is Unit V Risk Assessment / Risk Management. The unit will provide a definition of risk and the various components to determine a risk rating, review various approaches to determine risk, review a rating scale, and demonstrate how to use the scale to determine a risk rating.

VISUAL V-2



**Unit Objectives**

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


1. Explain what constitutes risk.
2. Evaluate risk using the Threat-Vulnerability Matrix (Risk Matrix poster) 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 of interest that should receive measures to mitigate vulnerabilities and reduce risk.

VISUAL V-3

**Risk Management**

Risk management is the deliberate process of understanding “risk” – the likelihood that a threat will harm an asset with some severity of consequences – and deciding on and implementing actions to reduce it.

GAO/NSIAD-98-74: Combating Terrorism – Threat and Risk Assessments Can Help Prioritize and Target Program Investments, April 1998



BUILDING DESIGN FOR HOMELAND SECURITY Unit V-3

**Risk Management**

Risk management incorporates an understanding of the vulnerability of assets to the consequences of threats and hazards.

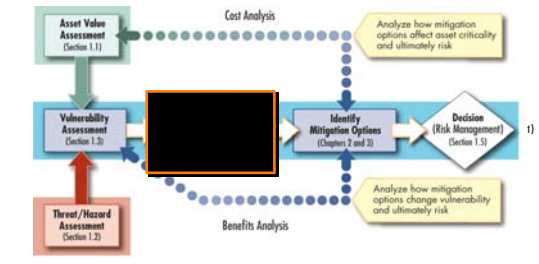
The objective is to reduce the vulnerability of assets through mitigation actions. Reducing vulnerabilities is the most straightforward approach to reducing risk.

However, realize that risk reduction has two other components, albeit not applicable to building design:


- Reduce asset value (Devalue the asset)
- Reduce threat (intelligence and law enforcement team to arrest terrorists before an attack can be carried out)

VISUAL V-4

**Assessment Flow Chart**



FEMA 426, Figure 1-3: The Assessment Process Model, p. 1-5



BUILDING DESIGN FOR HOMELAND SECURITY Unit V-4

**Assessment Flow Chart**

Reviewing the Assessment Flow Chart, the determination of quantitative risk values is the next step in the risk assessment process.

VISUAL V-5


**Definition of Risk**

Risk is a combination of:

- The probability that an event will occur, and
- The consequences of its occurrence

|                    | Low Risk | Medium Risk | High Risk |
|--------------------|----------|-------------|-----------|
| Risk Factors Total | 1-60     | 61-175      | > 176     |

$Risk = Asset\ Value \times Threat\ Rating \times Vulnerability\ Rating$



FEMA

FEMA 426, Table 1-19: Total Risk Color Code, p. 1-38  
BUILDING DESIGN FOR HOMELAND SECURITY Unit V-5

**Risk**

Risk can be defined as the potential for a loss or damage to an asset to occur. It takes into account the **value of an asset**, the **threats or hazards** that potentially impact the asset, and the **vulnerability** of the asset to the threat or hazard.

Values can be assigned to these three components of risk to provide a risk rating.


VISUAL V-6

**Quantifying Risk**

**Risk Assessment**

- Determine Asset Value
- Determine Threat Rating Value
- Determine Vulnerability Rating Value
- Determine relative risk for each threat against each asset

*Select mitigation measures that have the greatest benefit/cost for reducing risk*



FEMA

FEMA 426, Table 1-19: Total Risk Color Code, p. 1-38  
BUILDING DESIGN FOR HOMELAND SECURITY Unit V-6

**Quantifying Risk**

There are at least four steps or **required tasks** in the risk assessment process. A determination of the *Asset Value*, *Threat Rating Value*, *Vulnerability Rating Value*, and identifying or recommending appropriate *mitigation measures to reduce the risk*.

Determining the relative risk of threat against asset justifies the use of limited resources to reduce the greatest risk and focuses the mitigation measures needed.

**Exam Questions #A5 and B5**

VISUAL V-7

**An Approach to Quantifying Risk**

Risk = Asset Value x Threat Rating x Vulnerability Rating


Table 1-18: Risk Factors Definitions

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

Table 1-19: Total Risk Color Code

|                    |          |             |           |
|--------------------|----------|-------------|-----------|
|                    | Low Risk | Medium Risk | High Risk |
| Risk Factors Total | 1-60     | 61-175      | > 176     |

FEMA 426, p. 1-38  
BUILDING DESIGN FOR HOMELAND SECURITY Unit V-7




Exam Questions #A6 and B7

VISUAL V-8

**Critical Functions**

| Function              | Cyber attack | Armed attack (single gunman) | Vehicle bomb | CBR attack |
|-----------------------|--------------|------------------------------|--------------|------------|
| <b>Administration</b> | <b>280</b>   | <b>140</b>                   | <b>135</b>   | <b>90</b>  |
| Asset Value           | 5            | 5                            | 5            | 5          |
| Threat Rating         | 8            | 4                            | 3            | 2          |
| Vulnerability Rating  | 7            | 7                            | 9            | 9          |
| <b>Engineering</b>    | <b>128</b>   | <b>160</b>                   | <b>384</b>   | <b>144</b> |
| Asset Value           | 8            | 8                            | 8            | 8          |
| Threat Rating         | 8            | 5                            | 6            | 2          |
| Vulnerability Rating  | 2            | 4                            | 8            | 9          |

FEMA 426, Adaptation of Table 1-20: Site Functional Pre-Assessment Screening Matrix, p. 1-38  
BUILDING DESIGN FOR HOMELAND SECURITY Unit V-8



**An Approach to Quantifying Risk**

The risk assessment analyzes the threat, asset value, and vulnerability to ascertain the **level of risk** for each critical asset against each applicable threat.

An understanding of risk levels enables the owner of assets to prioritize and implement appropriate mitigation measures, paying particular attention to high consequence threats, to achieve the desired level of protection.

A simplified approach to quantifying risk is shown here. Values can be assigned to asset value/criticality, the threat or hazard, and vulnerability of the asset to the threats, and numerical scores can be determined that depict relative risk of these assets to manmade hazards. **(FEMA 426 Chapter 1, FEMA 452 Steps 1, 2, 3, and 4.)**

**Critical Functions Matrix**

This analysis completes the Critical Functions and the Critical Infrastructure Matrices that we saw in Units II, III, and IV.

The risk formula is applied and the numeric values color coded as discussed on the previous slide. The color code helps visualize the functions and infrastructure that are vulnerable and the scale helps to identify those areas for in-depth mitigation measures analysis.

The risk ratings under the Administration and Engineering Functions are highlighted. The numeric values result in Medium and High risk ratings for the Functions asset-threat/hazard pairs.



VISUAL V-9

### Critical Infrastructure

| Infrastructure            | Cyber attack | Armed attack (single gunman) | Vehicle bomb | CBR attack |
|---------------------------|--------------|------------------------------|--------------|------------|
| <b>Site</b>               | <b>48</b>    | <b>80</b>                    | <b>108</b>   | <b>72</b>  |
| Asset Value               | 4            | 4                            | 4            | 4          |
| Threat Rating             | 4            | 4                            | 3            | 2          |
| Vulnerability Rating      | 3            | 5                            | 9            | 9          |
| <b>Structural Systems</b> | <b>48</b>    | <b>128</b>                   | <b>192</b>   | <b>144</b> |
| Asset Value               | 8            | 8                            | 8            | 8          |
| Threat Rating             | 3            | 4                            | 3            | 2          |
| Vulnerability Rating      | 2            | 4                            | 8            | 9          |

FEMA 426, Adaptation of Table 1-21: Site Infrastructure Systems Pre-Assessment Screening Matrix, p. 1-39  
BUILDING DESIGN FOR HOMELAND SECURITY Unit V-9

**Critical Infrastructure Matrix**

The risk ratings under the Site and Structural Systems are highlighted. The numeric values result in Low to Medium risk ratings for the Infrastructure asset-threat/hazard pairs, except for Structural Systems – Vehicle Bomb which has a High risk rating.

VISUAL V-10

### Risk Assessment Results

| Function              | Cyber Attack | Armed Attack (single gunman) | Vehicle bomb | CBR Attack |
|-----------------------|--------------|------------------------------|--------------|------------|
| <b>Administration</b> | <b>36</b>    | <b>144</b>                   | <b>132</b>   | <b>96</b>  |
| Asset Value           | 3            | 3                            | 3            | 3          |
| Threat Rating         | 2            | 4                            | 3            | 3          |
| Vulnerability Rating  | 2            | 2                            | 3            | 3          |
| <b>Engineering</b>    | <b>120</b>   | <b>120</b>                   | <b>180</b>   | <b>144</b> |
| Asset Value           | 4            | 4                            | 4            | 4          |
| Threat Rating         | 3            | 4                            | 3            | 2          |
| Vulnerability Rating  | 2            | 4                            | 8            | 9          |
| <b>Manufacturing</b>  | <b>36</b>    | <b>36</b>                    | <b>36</b>    | <b>36</b>  |
| Asset Value           | 3            | 3                            | 3            | 3          |
| Threat Rating         | 2            | 4                            | 3            | 2          |
| Vulnerability Rating  | 2            | 3                            | 3            | 3          |
| <b>Data Center</b>    | <b>36</b>    | <b>120</b>                   | <b>144</b>   | <b>144</b> |
| Asset Value           | 4            | 4                            | 4            | 4          |
| Threat Rating         | 2            | 4                            | 3            | 3          |
| Vulnerability Rating  | 3            | 4                            | 9            | 9          |
| <b>Food Service</b>   | <b>3</b>     | <b>3</b>                     | <b>6</b>     | <b>36</b>  |
| Asset Value           | 1            | 1                            | 2            | 3          |
| Threat Rating         | 1            | 4                            | 3            | 2          |
| Vulnerability Rating  | 1            | 4                            | 9            | 9          |
| <b>Security</b>       | <b>36</b>    | <b>144</b>                   | <b>144</b>   | <b>120</b> |
| Asset Value           | 2            | 2                            | 2            | 2          |
| Threat Rating         | 4            | 4                            | 3            | 2          |
| Vulnerability Rating  | 5            | 3                            | 6            | 9          |
| <b>Manufacturing</b>  | <b>36</b>    | <b>64</b>                    | <b>60</b>    | <b>36</b>  |
| Asset Value           | 2            | 2                            | 2            | 2          |
| Threat Rating         | 4            | 4                            | 3            | 2          |
| Vulnerability Rating  | 1            | 8                            | 9            | 9          |
| <b>Day Care</b>       | <b>36</b>    | <b>36</b>                    | <b>36</b>    | <b>144</b> |
| Asset Value           | 3            | 3                            | 3            | 3          |
| Threat Rating         | 2            | 4                            | 3            | 2          |
| Vulnerability Rating  | 2            | 3                            | 3            | 9          |

\* VULNERABILITY RATING BASED ON TECHNICAL AND PRACTICE

FEMA 426, Table 1-20: Site Functional Pre-Assessment Screening Matrix, p. 1-38  
BUILDING DESIGN FOR HOMELAND SECURITY Unit V-10

**Risk Assessment Results**

The process is continued for all the asset-threat/hazard pairs of interest. This is a nominal example of a completed risk table.

The risk assessment results in a prioritized list of risks (i.e., asset – threat / hazard / vulnerability combinations) that can be used to select safeguards to reduce vulnerabilities (and risk) and to achieve a certain level of protection.

As stated previously, this subjective process is best applied to small organizations with few decision makers / decision levels. This subjective risk assessment process will probably not result in hard numbers that can be compared across different assessment teams, but the relative ranking of the asset-threat/hazard pairs on each team will have great correlation if both teams have consistent perspectives. Thus, the highest and lowest identified risks may not have the same rating numbers, but the same asset-threat/hazard pairs by the two teams will be close to identical. Divergence will occur if one team is concentrating on terrorism and

the other team is concentrating on continuity of business operations.

Large organizations require a more objective approach where the results of different assessment teams working independently can be compared by decision makers at many levels. These risk ratings will then be comparable across teams as to their numeric value, which is needed in a large organization.

In either case, the goal is to find where the application of limited resources will have the greatest benefit to reducing risk at the least cost.

### Selecting Mitigation Measures

In every design and renovation project, the owner ultimately has three choices when addressing the risk posed by terrorism. They can:


1. Do nothing and accept the risk (no cost).
2. Perform a risk assessment and manage the risk by installing reasonable mitigation measures (some cost).
3. Harden the building against all threats to achieve the least amount of risk (but at greatest cost).

### VISUAL V-11

**Selecting Mitigation Measures**

**Three Options:**

- Do nothing and accept the risk.
- Perform a risk assessment and manage the risk by installing reasonable mitigation measures.
- Harden the building against all threats to achieve the least amount of risk.



FEMA 426, Figure 1-13: Risk Management Choices, p. 1-44  
BUILDING DESIGN FOR HOMELAND SECURITY Unit V-11



### Exam Questions #A7 and B8

VISUAL V-12

**Mitigation Measures**

A mitigation measure is an action, device, or system used to reduce risk by affecting an asset, threat, or vulnerability.

- Regulatory measures
- Rehabilitation of existing structures
- Protective and control structures



BUILDING DESIGN FOR HOMELAND SECURITY Unit V-12

**Mitigation Measures**


After determining how specific threats potentially impact an asset (and occupants), the architect and building engineer can work with security and risk specialists to identify mitigation measures to reduce risk. Because it is not possible to completely eliminate risk, it is important to determine what level of protection is desirable, and the options for achieving this level through risk management.

VISUAL V-13

**Mitigation Measures**

Mitigation measures can be evaluated against the following parameters

- Political Support
- Community Acceptance
- Cost and Benefit
- Financial Resources
- Legal Authority
- Adversely Affected Population
- Adversely Effects on the Built Env.
- Environmental Impact
- Technical Capacity
- Maintenance and Operations
- Ease and Speed of Implementation
- Timeframe and Urgency
- Short-term and Long-Term Solutions
- Estimated Cost



BUILDING DESIGN FOR HOMELAND SECURITY Unit V-13

**Measures to Reduce Risk**

Higher risk hazards require mitigation measures to reduce risk. Mitigation measures are conceived by the design professional and are best incorporated into the building architecture, building systems, and operational parameters, with consideration for life-cycle costs.

There are many factors that impact what mitigation measures can be implemented at low, medium, and high levels of difficulty.

In some cases, mitigation measures to enhance security may be in conflict with other design intentions, building codes, planning board master plans, etc.

VISUAL V-14

**Achieving Building Security:  
Planning Factors**

Building security integrates multiple concepts and practices.

Objective is to achieve a balanced approach that combines aesthetics, enhanced security, and use of non-structural measures.



BUILDING DESIGN FOR HOMELAND SECURITY Unit V-14

**Achieving Building Security**

The assessment process provides concepts for integrating land use planning, landscape architecture, site planning, and other strategies to mitigate the Design Basis Threats as identified in the risk assessment.

Integrating security measures into design and/or maintenance of buildings presents the asset owner with multiple opportunities of achieving a balance among many objectives such as reducing risk; facilitating proper building function; aesthetics and matching architecture; hardening of physical structures beyond required building codes and standards; and maximizing use of non-structural systems.

[The last point tries to illustrate that the balanced approach to building security tries not to place everything into hardening the structure to deny the consequences to the terrorist's tactics. Thus, non-structural systems, especially in renovation projects, may provide a level of risk reduction comparable to structural hardening but at a must reduced cost or at a more timely implementation.]

VISUAL V-15

**Process Review**

**Calculate** the relative risk for each threat against each asset

**Identify** the high risk areas

**Identify** Mitigation Options to reduce the risk



BUILDING DESIGN FOR HOMELAND SECURITY Unit V-15

**Process Review**

- Calculate the relative risk for each threat against each asset
- Identify the high risk areas
- Identify Mitigation Options to reduce the risk

To get the maximum benefit from limited resources, realize that certain mitigation measures can reduce risk for multiple, high-risk asset – threat / hazard pairs.

INSTRUCTOR NOTES

CONTENT/ACTIVITY

VISUAL V-16


**Summary**

Risk Definition

Critical Function and Critical Infrastructure Matrices

Numerical and color-coded risk scale

Identify Mitigation Options



BUILDING DESIGN FOR HOMELAND SECURITY Unit V-16

**Summary**

- Risk Definition
- Critical Function and Critical Infrastructure Matrices
- Numerical and Color-coded Risk Scale
- Identify Mitigation Options

VISUAL V-17

**Unit V Case Study Activity**

**Risk Rating**

**Background**

Formula for determining a numeric value risk for each asset-threat/hazard pair:


**Risk = Asset Value x Threat Rating x Vulnerability Rating**

**Requirements: Vulnerability Rating Approach**

Use worksheet tables to summarize Case Study asset, threat, and vulnerability ratings conducted in the previous activities

Use the risk formula to determine the risk rating for each asset-threat/hazard pair for:

- Critical Functions
- Critical Infrastructure



BUILDING DESIGN FOR HOMELAND SECURITY Unit V-17

**Student Activity**

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:

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

**Activity Requirements**

Working in small groups, use the worksheet tables to summarize the asset, threat and vulnerability assessments conducted in the previous three unit student activities for the selected Case Study.

Then use the risk formula to determine the risk rating for each asset-threat/hazard pair identified under Critical Functions and under Critical Infrastructure.

Take 15 minutes to complete this activity.

Refer participants to the Unit V Case Study activity in the Student Manual.

Members of the instructor staff should be available to answer questions and assist groups as needed.

At the end of 15 minutes, reconvene the class and facilitate group reporting (plenary group will take about 10 minutes).

**INSTRUCTOR NOTES**

**CONTENT/ACTIVITY**

Solutions will be reviewed in plenary group.

**Transition**

Unit VI tomorrow morning will provide an alternate to performing this risk assessment process manually as you have done today in your student activities.

**UNIT V-A CASE STUDY ACTIVITY:  
RISK RATING  
(Suburban Version)**

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

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

**Requirements**

1. 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 of interest identified under Critical Functions and under Critical Infrastructure. Transfer to the Risk Matrix and reach team consensus on answers.
2. Identify the highest risk ratings and use **Figure 1-13 of FEMA 426 (page 1-44)** to begin a determination of the risk management options available to reduce these risk ratings by reducing applicable individual ratings for asset value, threat/hazard, or vulnerability. Then identify the top three risk ratings and keep in mind as mitigation measures are discussed in future instruction units.

**HIC Critical Functions Risk Rating**

| Function   | Cyber Attack | Armed Attack | Vehicle Bomb | CBR Attack |
|--|--------------|--------------|--------------|------------|
| <b>1. Administration<br/>Risk Rating</b>                 | <b>128</b>   | <b>96</b>    | <b>192</b>   | <b>96</b>  |
| Asset Value  | 4            | 4            | 4            | 4          |
| Threat Rating  | 8            | 3            | 6            | 4          |
| Vulnerability Rating                                     | 4            | 8            | 8            | 6          |
| <b>2. Engineering/IT<br/>Technicians<br/>Risk Rating</b> | <b>160</b>   | <b>90</b>    | <b>240</b>   | <b>120</b> |
| Asset Value  | 5            | 5            | 5            | 5          |
| Threat Rating  | 8            | 3            | 6            | 4          |
| Vulnerability Rating                                     | 4            | 6            | 8            | 6          |
| <b>3. Loading Dock/<br/>Warehouse<br/>Risk Rating</b>    | <b>80</b>    | <b>120</b>   | <b>240</b>   | <b>120</b> |
| Asset Value  | 5            | 5            | 5            | 5          |
| Threat Rating  | 8            | 3            | 6            | 4          |
| Vulnerability Rating                                     | 2            | 8            | 8            | 6          |
| <b>4. Data Center<br/>Risk Rating</b>                    | <b>240</b>   | <b>120</b>   | <b>480</b>   | <b>240</b> |

| Function                             | Cyber Attack | Armed Attack | Vehicle Bomb | CBR Attack |
|--------------------------------------|--------------|--------------|--------------|------------|
| Asset Value                          | 10           | 10           | 10           | 10         |
| Threat Rating                        | 8            | 3            | 6            | 4          |
| Vulnerability Rating                 | 3            | 4            | 8            | 6          |
| <b>5. Communications Risk Rating</b> | <b>192</b>   | <b>96</b>    | <b>384</b>   | <b>192</b> |
| Asset Value                          | 8            | 8            | 8            | 8          |
| Threat Rating                        | 8            | 3            | 6            | 4          |
| Vulnerability Rating                 | 3            | 4            | 8            | 6          |
| <b>6. Security Risk Rating</b>       | <b>224</b>   | <b>168</b>   | <b>336</b>   | <b>168</b> |
| Asset Value                          | 7            | 7            | 7            | 7          |
| Threat Rating                        | 8            | 3            | 6            | 4          |
| Vulnerability Rating                 | 4            | 8            | 8            | 6          |
| <b>7. Housekeeping Risk Rating</b>   | <b>16</b>    | <b>6</b>     | <b>48</b>    | <b>24</b>  |
| Asset Value                          | 1            | 1            | 1            | 1          |
| Threat Rating                        | 8            | 3            | 6            | 4          |
| Vulnerability Rating                 | 2            | 2            | 8            | 6          |

**HIC Critical Infrastructure Risk Rating**

| Infrastructure                           | Cyber Attack | Armed Attack | Vehicle Bomb | CBR Attack |
|--|--------------|--------------|--------------|------------|
| <b>1. Site Risk Rating</b>               | <b>5</b>     | <b>120</b>   | <b>240</b>   | <b>160</b> |
| Asset Value                              | 5            | 5            | 5            | 5          |
| Threat Rating                            | 1            | 3            | 6            | 4          |
| Vulnerability Rating                     | 1            | 8            | 8            | 6          |
| <b>2. Architectural Risk Rating</b>      | <b>5</b>     | <b>120</b>   | <b>240</b>   | <b>20</b>  |
| Asset Value                              | 5            | 5            | 5            | 5          |
| Threat Rating                            | 1            | 3            | 6            | 4          |
| Vulnerability Rating                     | 1            | 8            | 8            | 1          |
| <b>3. Structural Systems Risk Rating</b> | <b>5</b>     | <b>120</b>   | <b>240</b>   | <b>20</b>  |
| Asset Value                              | 5            | 5            | 5            | 5          |
| Threat Rating                            | 1            | 3            | 6            | 4          |
| Vulnerability Rating                     | 1            | 8            | 8            | 1          |



| <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>           | <b>5</b>            | <b>120</b>          | <b>240</b>          | <b>20</b>         |
| Asset Value                                      | 5                   | 5                   | 5                   | 5                 |
| Threat Rating                                    | 1                   | 3                   | 6                   | 4                 |
| Vulnerability Rating                             | 1                   | 8                   | 8                   | 1                 |
| <b>5. Utility Systems Risk Rating</b>            | <b>125</b>          | <b>175</b>          | <b>180</b>          | <b>20</b>         |
| Asset Value                                      | 5                   | 5                   | 5                   | 5                 |
| Threat Rating                                    | 5                   | 5                   | 6                   | 4                 |
| Vulnerability Rating                             | 5                   | 7                   | 6                   | 1                 |
| <b>6. Mechanical Systems Risk Rating</b>         | <b>175</b>          | <b>245</b>          | <b>336</b>          | <b>196</b>        |
| Asset Value                                      | 7                   | 7                   | 7                   | 7                 |
| Threat Rating                                    | 5                   | 5                   | 6                   | 4                 |
| Vulnerability Rating                             | 5                   | 7                   | 8                   | 7                 |
| <b>7. Plumbing and Gas Systems Risk Rating</b>   | <b>5</b>            | <b>45</b>           | <b>240</b>          | <b>20</b>         |
| Asset Value                                      | 5                   | 5                   | 5                   | 5                 |
| Threat Rating                                    | 1                   | 3                   | 6                   | 4                 |
| Vulnerability Rating                             | 1                   | 3                   | 8                   | 1                 |
| <b>8. Electrical Systems Risk Rating</b>         | <b>175</b>          | <b>147</b>          | <b>336</b>          | <b>140</b>        |
| Asset Value                                      | 7                   | 7                   | 7                   | 7                 |
| Threat Rating                                    | 5                   | 3                   | 6                   | 4                 |
| Vulnerability Rating                             | 5                   | 7                   | 8                   | 5                 |
| <b>9. Fire Alarm Systems Risk Rating</b>         | <b>30</b>           | <b>45</b>           | <b>240</b>          | <b>60</b>         |
| Asset Value                                      | 5                   | 5                   | 5                   | 5                 |
| Threat Rating                                    | 2                   | 3                   | 6                   | 4                 |
| Vulnerability Rating                             | 3                   | 3                   | 8                   | 3                 |
| <b>10. IT/Communications Systems Risk Rating</b> | <b>400</b>          | <b>120</b>          | <b>480</b>          | <b>240</b>        |
| Asset Value                                      | 10                  | 10                  | 10                  | 10                |
| Threat Rating                                    | 10                  | 3                   | 6                   | 4                 |
| Vulnerability Rating                             | 4                   | 4                   | 8                   | 6                 |

**UNIT V-B CASE STUDY ACTIVITY:  
RISK RATING  
(Urban Version)**

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

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

**Requirements**

1. Use the following tables to summarize the HZC 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 of interest identified under Critical Functions and under Critical Infrastructure. Transfer to the Risk Matrix and reach team consensus on answers.

2. Identify the highest risk ratings and use **Figure 1-13 of FEMA 426 (page 1-44)** to begin a determination of the risk management options available to reduce these risk ratings by reducing applicable individual ratings for asset value, threat/hazard, or vulnerability. Then identify the top three risk ratings and keep in mind as mitigation measures are discussed in future instruction units.

**HZC Critical Functions Risk Rating**

| Function   | Cyber Attack | Armed Attack | Vehicle Bomb | CBR Attack |
|--|--------------|--------------|--------------|------------|
| <b>8. Administration<br/>Risk Rating</b>                 | <b>210</b>   | <b>252</b>   | <b>630</b>   | <b>252</b> |
| Asset Value  | 7            | 7            | 7            | 7          |
| Threat Rating  | 6            | 6            | 9            | 6          |
| Vulnerability Rating                                     | 5            | 6            | 10           | 6          |
| <b>9. Engineering/IT<br/>Technicians<br/>Risk Rating</b> | <b>144</b>   | <b>96</b>    | <b>648</b>   | <b>240</b> |
| Asset Value  | 8            | 8            | 8            | 8          |
| Threat Rating  | 6            | 4            | 9            | 6          |
| Vulnerability Rating                                     | 3            | 3            | 9            | 5          |

| Function   | Cyber Attack | Armed Attack | Vehicle Bomb | CBR Attack |
|--|--------------|--------------|--------------|------------|
| <b>10. Loading Dock/<br/>Warehouse<br/>Risk Rating</b> | <b>60</b>    | <b>210</b>   | <b>450</b>   | <b>210</b> |
| Asset Value  | 5            | 5            | 5            | 5          |
| Threat Rating  | 6            | 7            | 9            | 6          |
| Vulnerability Rating                                   | 2            | 6            | 10           | 7          |
| <b>11. Data Center<br/>Risk Rating</b>                 | <b>420</b>   | <b>90</b>    | <b>900</b>   | <b>300</b> |
| Asset Value  | 10           | 10           | 10           | 10         |
| Threat Rating  | 6            | 3            | 9            | 6          |
| Vulnerability Rating                                   | 7            | 3            | 10           | 5          |
| <b>12. Communications<br/>Risk Rating</b>              | <b>336</b>   | <b>96</b>    | <b>720</b>   | <b>240</b> |
| Asset Value  | 8            | 8            | 8            | 8          |
| Threat Rating  | 6            | 4            | 9            | 6          |
| Vulnerability Rating                                   | 7            | 3            | 10           | 5          |
| <b>13. Security<br/>Risk Rating</b>                    | <b>168</b>   | <b>196</b>   | <b>360</b>   | <b>168</b> |
| Asset Value  | 4            | 4            | 4            | 4          |
| Threat Rating  | 6            | 7            | 9            | 6          |
| Vulnerability Rating                                   | 7            | 7            | 10           | 7          |
| <b>14. Housekeeping<br/>Risk Rating</b>                | <b>4</b>     | <b>8</b>     | <b>144</b>   | <b>60</b>  |
| Asset Value  | 2            | 2            | 2            | 2          |
| Threat Rating  | 2            | 2            | 9            | 6          |
| Vulnerability Rating                                   | 1            | 2            | 8            | 5          |

**HZC Critical Infrastructure Risk Rating**

| <b>Infrastructure</b>                     | <b>Cyber Attack</b> | <b>Armed Attack</b> | <b>Vehicle Bomb</b> | <b>CBR Attack</b> |
|---|---------------------|---------------------|---------------------|-------------------|
| <b>11. Site Risk Rating</b>               | <b>10</b>           | <b>75</b>           | <b>405</b>          | <b>270</b>        |
| Asset Value                               | 5                   | 5                   | 5                   | 5                 |
| Threat Rating                             | 1                   | 3                   | 9                   | 6                 |
| Vulnerability Rating                      | 2                   | 5                   | 9                   | 9                 |
| <b>12. Architectural Risk Rating</b>      | <b>7</b>            | <b>105</b>          | <b>630</b>          | <b>210</b>        |
| Asset Value                               | 7                   | 7                   | 7                   | 7                 |
| Threat Rating                             | 1                   | 3                   | 9                   | 6                 |
| Vulnerability Rating                      | 1                   | 5                   | 10                  | 5                 |
| <b>13. Structural Systems Risk Rating</b> | <b>8</b>            | <b>24</b>           | <b>720</b>          | <b>32</b>         |
| Asset Value                               | 8                   | 8                   | 8                   | 8                 |
| Threat Rating                             | 1                   | 3                   | 9                   | 4                 |
| Vulnerability Rating                      | 1                   | 1                   | 10                  | 1                 |
| <b>14. Envelope Systems Risk Rating</b>   | <b>7</b>            | <b>126</b>          | <b>630</b>          | <b>42</b>         |
| Asset Value                               | 7                   | 7                   | 7                   | 7                 |
| Threat Rating                             | 1                   | 3                   | 9                   | 6                 |
| Vulnerability Rating                      | 1                   | 6                   | 10                  | 1                 |
| <b>15. Utility Systems Risk Rating</b>    | <b>40</b>           | <b>24</b>           | <b>576</b>          | <b>46</b>         |
| Asset Value                               | 8                   | 8                   | 8                   | 8                 |
| Threat Rating                             | 1                   | 3                   | 9                   | 6                 |
| Vulnerability Rating                      | 5                   | 1                   | 8                   | 1                 |

| <b>Infrastructure</b>                            | <b>Cyber Attack</b> | <b>Armed Attack</b> | <b>Vehicle Bomb</b> | <b>CBR Attack</b> |
|--|---------------------|---------------------|---------------------|-------------------|
| <b>16. Mechanical Systems Risk Rating</b>        | <b>160</b>          | <b>48</b>           | <b>504</b>          | <b>336</b>        |
| Asset Value                                      | 8                   | 8                   | 8                   | 8                 |
| Threat Rating                                    | 5                   | 3                   | 9                   | 6                 |
| Vulnerability Rating                             | 4                   | 2                   | 7                   | 7                 |
| <b>17. Plumbing and Gas Systems Risk Rating</b>  | <b>32</b>           | <b>32</b>           | <b>504</b>          | <b>144</b>        |
| Asset Value                                      | 8                   | 8                   | 8                   | 8                 |
| Threat Rating                                    | 1                   | 3                   | 9                   | 6                 |
| Vulnerability Rating                             | 4                   | 1                   | 7                   | 3                 |
| <b>18. Electrical Systems Risk Rating</b>        | <b>160</b>          | <b>120</b>          | <b>648</b>          | <b>144</b>        |
| Asset Value                                      | 8                   | 8                   | 8                   | 8                 |
| Threat Rating                                    | 5                   | 5                   | 9                   | 6                 |
| Vulnerability Rating                             | 4                   | 3                   | 9                   | 3                 |
| <b>19. Fire Alarm Systems Risk Rating</b>        | <b>64</b>           | <b>16</b>           | <b>504</b>          | <b>96</b>         |
| Asset Value                                      | 8                   | 8                   | 8                   | 8                 |
| Threat Rating                                    | 2                   | 2                   | 9                   | 6                 |
| Vulnerability Rating                             | 4                   | 1                   | 7                   | 2                 |
| <b>20. IT/Communications Systems Risk Rating</b> | <b>576</b>          | <b>64</b>           | <b>720</b>          | <b>144</b>        |
| Asset Value                                      | 8                   | 8                   | 8                   | 8                 |
| Threat Rating                                    | 8                   | 4                   | 9                   | 6                 |
| Vulnerability Rating                             | 9                   | 2                   | 10                  | 3                 |

*This page intentionally left blank*