Unit III

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 – FEMA, 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 threat rating of the four threats selected for this course (Cyber Attack, Armed Attack, Vehicle Bomb, CBR Attack) against each identified asset using the Case Study.

REFERENCES

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, pages 1-14 to 1-24
2. FEMA 452, *Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings*, pages 1-1 to 1-30
3. Case Study – Appendix A: Suburban, Hazardville Information Company or Appendix B: Urban, HazardCorp Building as selected
4. Student Manual, Unit III-A or Unit III-B as selected (info only – not in SM)
5. Unit III visuals (info only – not in SM)

REQUIREMENTS

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

UNIT III OUTLINE

2. Steps to the Threat Selection and Rating Process	6 minutes	IG III-10
3. Threat Sources, Design Basis Threat, and Levels of Protection	11 minutes	IG III-15
4. Summary, Student Activity, and Transition	2 minutes	IG III-22
5. Activity: Threat / Hazard Rating (Version **A Suburban**) [30 minutes for students, 15 minutes for instructor review or as adjusted based upon how long Items 1 to 5 took above])	45 minutes	IG III-A-25
6. Activity: Threat / Hazard Rating (Version **B Urban**) [30 minutes for students, 15 minutes for instructor review or as adjusted based upon how long Items 1 to 5 took above]	45 minutes	IG III-B-32

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. However, Local Area discussion may be generated as students have specific situations for which they would like to determine threat rating or their own experiences in trying to obtain threat and threat rating information in their Local Area.

  The Instructor will begin this unit with a brief discussion of terrorism and technological hazards worldwide and within the United States. The probability of natural hazards and how they are considered during design will be compared to the probability of manmade hazards, both terrorism and technological accidents. This sets the stage for identifying where to get information about threats and hazards.

  Next, the Instructor will use **FEMA 386-7** to describe the spectrum of tactics or events that can occur. This leads into the five components used to define a threat (or hazard).

  A simplified threat rating approach will be presented that can be used during a design charette for new construction or major renovation. This **FEMA 426** approach forms the basis of the Unit III student activity.

- **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 Unit III student activity begins with a threat definition or threat score for a 500-pound vehicle bomb using **FEMA 452 Table 1-4** criteria as Step 1 of the process. Then Step 2 has the students applying the techniques (threat identification, threat description, and threat rating) to the Case Study to identify and rate the threat from cyber attack, armed attack, explosive blast, and agents (chemical, biological, and radiological) against the assets identified and rated in the previous student activity. Note that these event profiles can result from terrorism, criminal activity, or technological hazards.

- 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 threat / hazard ratings determined by the team must be transferred to the Risk Matrix poster.

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

- While students are working, <u>all</u> instructors should closely observe the groups' process and progress. If any groups are struggling, immediately assist them by clarifying the assignment and providing as much help as is necessary for the groups to complete the requirement in the allotted time. Also, monitor each group for full participation of all members. For example, ask any student who is not fully engaged a question that requires his/her viewpoint to be presented to the group.

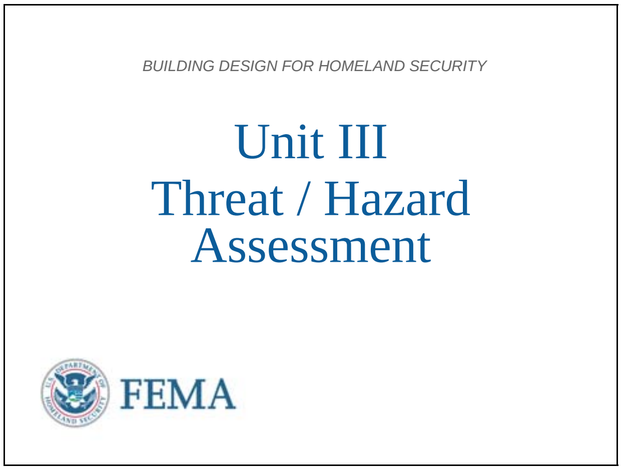
- At the end of the working period, reconvene the class.

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

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

- Ask for and answer questions.

VISUAL III-1



BUILDING DESIGN FOR HOMELAND SECURITY

Unit III
Threat / Hazard Assessment

FEMA

The students will apply these techniques (threat identification, threat description, and threat rating) to the Case Study to identify and rate the threat from explosive blast and agents (chemical, biological, and radiological). Note that these event profiles can result from terrorism or technological hazards. They will also rate the threat for Cyber Terrorism and Armed Attack.

Introduction and Unit Overview

This is Unit III Threat / Hazard Assessment. The unit starts with a brief discussion of terrorism and technological hazards worldwide and within the United States. The probability of natural hazards and how they are considered during design will be compared to the probability of manmade hazards, both terrorism and technological accidents.

The five components used to define a threat (or hazard) is taken from an approach developed by the US Marshals Service and is used to illustrate how assessment analysis can be coupled with increasing threat levels.

VISUAL III-2

Unit Objectives

Identify the threats and hazards that may impact a building or site.

Define each threat and hazard using the FEMA 426 methodology.

Provide a numerical rating for the threat or hazard and justify the basis for the rating.

Define the Design Basis Threat, Levels of Protection, and Layers of Defense.

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY Unit III-2

Unit Objectives

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

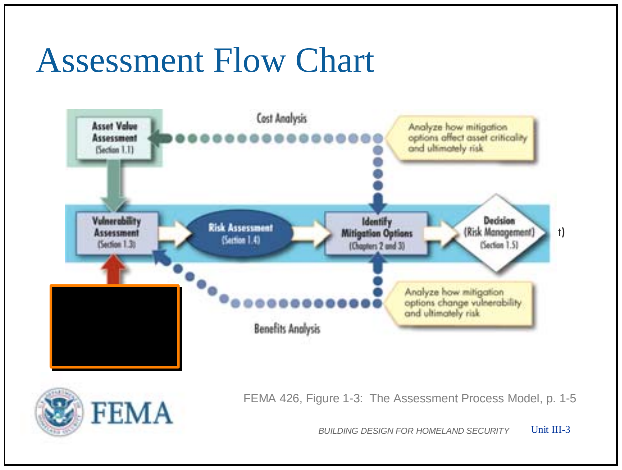
1. Identify the threats and hazards that may impact a building or site.

2. Define each threat and hazard using the **FEMA 426** methodology.

3. Provide a numerical rating for the threat or hazard and justify the basis for the rating.

4. Define the Design Basis Threat, Levels of Protection, and Layers of Defense.

VISUAL III-3



Assessment Flow Chart

Asset Value Assessment (Section 1.1)
Cost Analysis
Analyze how mitigation options affect asset criticality and ultimately risk
Vulnerability Assessment (Section 1.3)
Risk Assessment (Section 1.4)
Identify Mitigation Options (Chapters 2 and 3)
Decision (Risk Management) (Section 1.5)
t)
Analyze how mitigation options change vulnerability and ultimately risk
Benefits Analysis

[redacted]

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

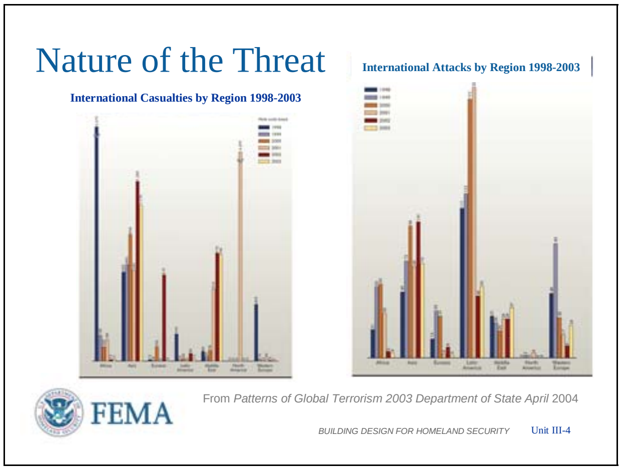
FEMA

BUILDING DESIGN FOR HOMELAND SECURITY Unit III-3

Assessment Flow Chart

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

VISUAL III-4



Nature of the Threat

FEMA

From *Patterns of Global Terrorism 2003 Department of State April* 2004

BUILDING DESIGN FOR HOMELAND SECURITY Unit III-4

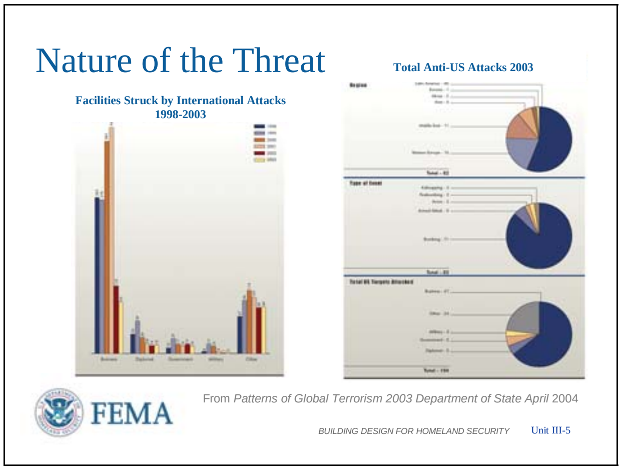
Nature of the Threat (1/3)

With enhanced migration of terrorist groups from conflict-ridden countries, the formation of extensive international terrorist infrastructures and the increased reach of terrorist groups, terrorism has become a global concern.

Terrorism and physical attacks on buildings have continued to increase in the past decade. The geographical isolation of the United States is not a sufficient barrier to prevent an attack on U.S. cities and citizens. These data in this and the next two slides from the Department of State and FBI shows these trends and demonstrate the far reaching incidents and diverse natures and targets of recent terrorist attacks.

For example, his slide shows the varying trends of attacks and casualties by continent around the world. Some trends are up, some are down, but the presence and capability is there.

VISUAL III-5



Nature of the Threat

Facilities Struck by International Attacks
1998-2003

Total Anti-US Attacks 2003

From *Patterns of Global Terrorism 2003 Department of State April* 2004

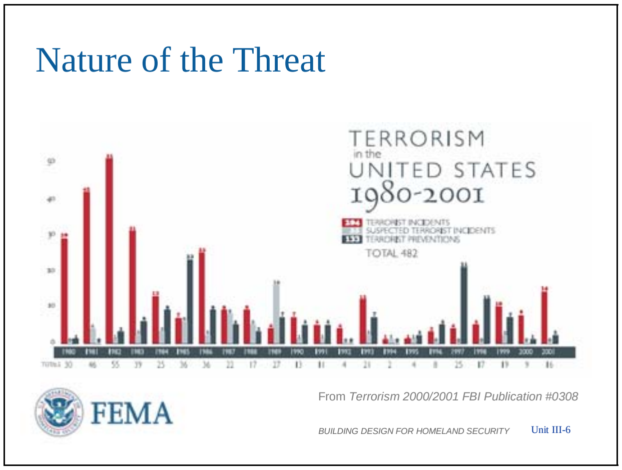
BUILDING DESIGN FOR HOMELAND SECURITY Unit III-5

Nature of the Threat (2/3)

This slide illustrates Anti-US attacks are predominantly NOT against diplomatic, government, and military targets, but against <u>business and others</u>.

Also the predominant Anti-US tactic used was <u>bombing</u> over this reporting period.

VISUAL III-6



Nature of the Threat

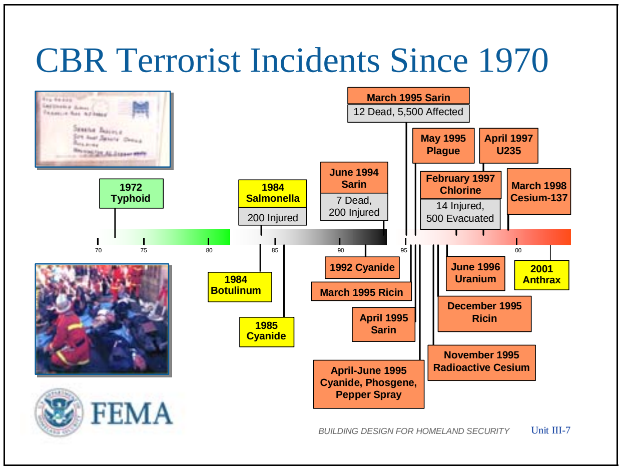
From *Terrorism 2000/2001 FBI Publication #0308*

BUILDING DESIGN FOR HOMELAND SECURITY Unit III-6

Nature of the Threat (3/3)

Finally, this slide illustrates that incidents of terrorism inside the US is generally going down, but the incidents that have occurred to the right of this chart over this 22 year period are especially horrific.

VISUAL III-7



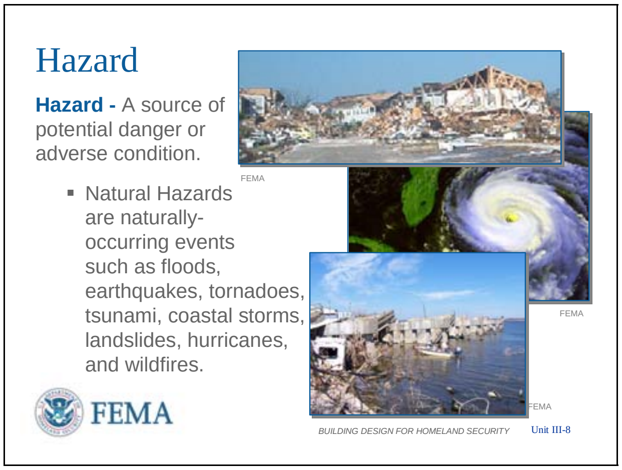
CBR Terrorist Incidents Since 1970

BUILDING DESIGN FOR HOMELAND SECURITY Unit III-7

CBR Terrorist Incidents Since 1970

- CBR attacks have been used since ancient times and, in the past 20 years, over 50 attacks have occurred.
- CBR attacks require the right weather, population, and dispersion to be effective.
- Recent attacks have had limited effectiveness or have been conducted on a relatively small scale.
- Future attacks with Weapons of Mass Destruction could occur on a regional or global scale.

VISUAL III-8



Hazard

Hazard - A source of potential danger or adverse condition.

- Natural Hazards are naturally-occurring events such as floods, earthquakes, tornadoes, tsunami, coastal storms, landslides, hurricanes, and wildfires.

FEMA

FEMA

FEMA

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY Unit III-8

Hazard

- **Hazard -** A source of potential danger or adverse condition.

- **Natural Hazards** are naturally-occurring events such as floods, earthquakes, tornadoes, tsunami, coastal storms, landslides, hurricanes, and wildfires.
- A natural event is a hazard when it has the potential to harm people or property (FEMA 386-2, *Understanding Your Risks*).
- The risks of natural hazards may be increased or decreased as a result of human activity. (Like building in a floodplain (bad) or hardening for hurricanes (good))

VISUAL III-9

Manmade Threats

Threats – Any indication, circumstance, or event with the potential to cause loss of, or damage to an asset. They can be technological accidents and terrorist attacks.

Technological accident

Terrorism act

FEMA

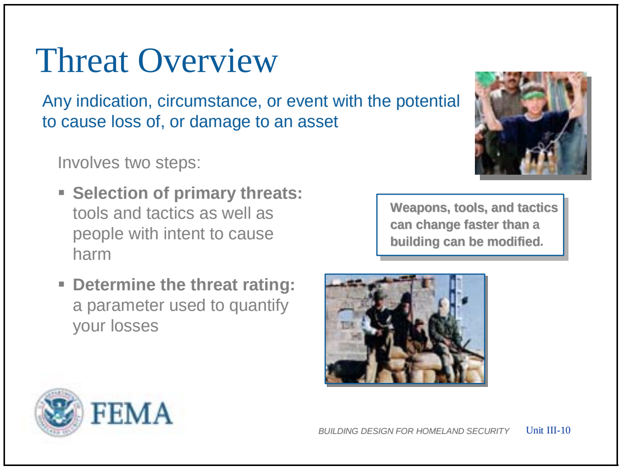
BUILDING DESIGN FOR HOMELAND SECURITY Unit III-9

Manmade Threats/Hazards

- **Technological Accidents** are incidents that can arise from human activities such as manufacturing, transportation, storage, and use of hazardous materials. For the sake of simplicity, it is assumed that technological emergencies are accidental and that their consequences are unintended.

- **Terrorism** is the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. (28 CFR, Section 0.85)

VISUAL III-10



Threat Overview

Any indication, circumstance, or event with the potential to cause loss of, or damage to an asset

Involves two steps:

- **Selection of primary threats:** tools and tactics as well as people with intent to cause harm
- **Determine the threat rating:** a parameter used to quantify your losses

Weapons, tools, and tactics can change faster than a building can be modified.

FEMA

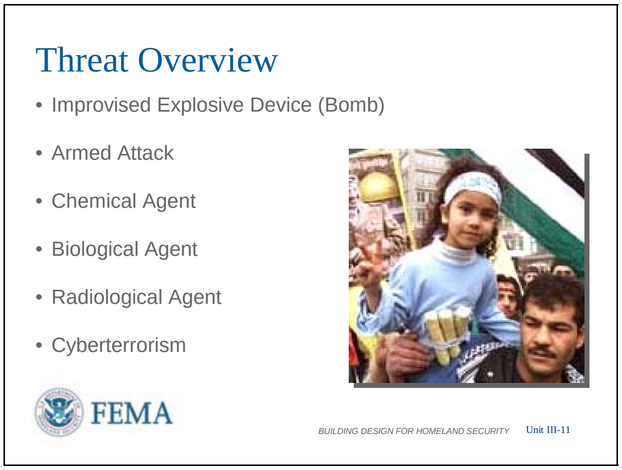
BUILDING DESIGN FOR HOMELAND SECURITY Unit III-10

Two-Step Process

A two-step process is utilized to complete the threat assessment.

- The first step is the selection of the primary threats that may affect your building.
- The second is the determination of the threat rating.

VISUAL III-11



Threat Overview

- Improvised Explosive Device (Bomb)
- Armed Attack
- Chemical Agent
- Biological Agent
- Radiological Agent
- Cyberterrorism

FEMA

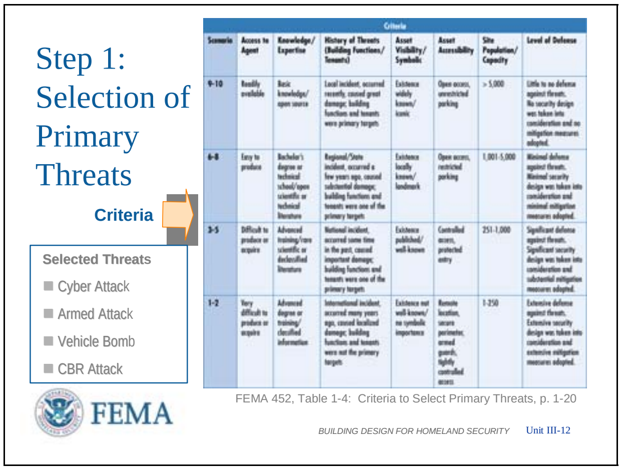
BUILDING DESIGN FOR HOMELAND SECURITY Unit III-11

Identify Each Threat / Hazard

- **Table 1-3 in FEMA 426 (page 1-17)** outlines the broad spectrum of terrorist threats and technological hazards. Some of the items are listed here.

- While we can think of terrorist tactics and technological hazards (such as HazMat releases), a runaway truck crashing into a power line, a storage tank, or a telephone pedestal can be equally detrimental. Similarly, surveillance of a company's operations may divulge company trade secrets that are detrimental to the company's economic bottom line or an industry in a country.

VISUAL III-12



Step 1: Selection of Primary Threats

Criteria

Selected Threats

- Cyber Attack
- Armed Attack
- Vehicle Bomb
- CBR Attack

	Criteria						
Scenario	Access to Agent	Knowledge/ Expertise	History of Threats (Building Functions/ Tenants)	Asset Visibility/ Symbolic	Asset Accessibility	Site Population/ Capacity	Level of Defense
9-10	Readily available	Basic knowledge/ open source	Local incident, occurred recently, caused great damage; building functions and tenants were primary targets	Existence widely known/ iconic	Open access, unrestricted parking	> 5,000	Little to no defense against threats. No security design was taken into consideration and no mitigation measures adopted.
6-8	Easy to produce	Bachelor's degree or technical school/open scientific or technical literature	Regional/State incident, occurred a few years ago, caused substantial damage; building functions and tenants were one of the primary targets	Existence locally known/ landmark	Open access, restricted parking	1,001-5,000	Minimal defense against threats. Minimal security design was taken into consideration and minimal mitigation measures adopted.
3-5	Difficult to produce or acquire	Advanced training/rare scientific or declassified literature	National incident, occurred some time in the past, caused important damage; building functions and tenants were one of the primary targets	Existence published/ well-known	Controlled access, protected entry	251-1,000	Significant defense against threats. Significant security design was taken into consideration and substantial mitigation measures adopted.
1-2	Very difficult to produce or acquire	Advanced degree or training/ classified information	International incident, occurred many years ago, caused localized damage; building functions and tenants were not the primary targets	Existence not well-known/ no symbolic importance	Remote location, secure perimeter, armed guards, tightly controlled access	1-250	Extensive defense against threats. Extensive security design was taken into consideration and extensive mitigation measures adopted.

FEMA 452, Table 1-4: Criteria to Select Primary Threats, p. 1-20

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY Unit III-12

Step 1: Selection of Primary Threats

To select the primary threats, the selected criteria outlined on this slide are designed to help you to rank potential threats from 1-10 (10 being the greater threat).

- **Access to Agent:** The access to agent is the ease by which the source material can be acquired to carry out the attack. Consideration includes the local HazMat inventory, farm and mining supplies, major chemical or manufacturing plants, university and commercial laboratories, and transportation centers.

- **Knowledge/Expertise:** The general level of skill and training that combines the ability to create the weapon (or weaponize an agent) and the technical knowledge of the systems to be attacked (HVAC, nuclear, etc.). Knowledge and expertise can be gained by surveillance, open source research, specialized training, or years of practice in industry.

- **History of Threats Against Buildings:** What has the potential threat element done in the past and how many times? When was the most recent incident and where, and against what target? What tactics did they use?

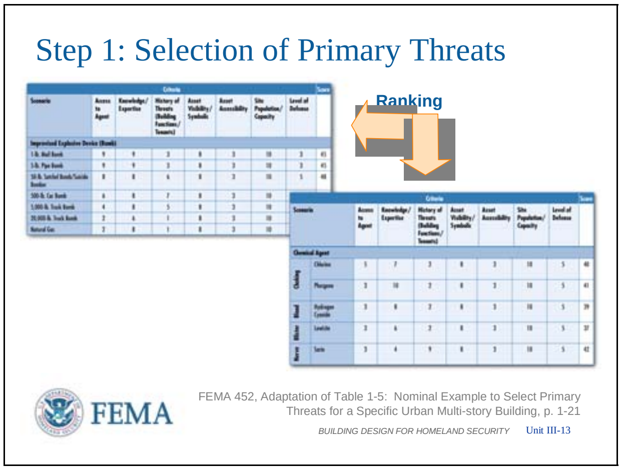
- **Asset Visibility/Symbolic:** The economic, cultural, and symbolic importance of the building to society that may be exploited by the terrorist seeking to cause monetary or political gain through their actions.

- **Asset Accessibility:** The ability of the terrorist to become well-positioned to carry out an attack at the critical location against the intended target. The critical location is a function of the site, the building layout, and the security measures in place.

- **Site Population/Capacity:** The population demographics of the building and surrounding area.

- **Level of Defense:** What security measures are in place and how effective are they against the available tactics currently in use?

VISUAL III-13



Step 1: Selection of Primary Threats

Scenario	Criteria							Score
	Access to Agent	Knowledge/ Expertise	History of Threats (Building Functions/ Tenants)	Asset Visibility/ Symbolic	Asset Accessibility	Site Population/ Capacity	Level of Defense	
Improvised Explosive Device (Bomb)								
1-lb. Mail Bomb	9	9	3	8	3	10	3	45
5-lb. Pipe Bomb	9	9	3	8	3	10	3	45
50-lb. Satchel Bomb/Suicide Bomber	8	8	6	8	3	10	5	48
500-lb. Car Bomb	6	8	7	8	3	10		
1,000-lb. Truck Bomb	4	8	5	8	3	10		
20,000-lb. Truck Bomb	2	6	1	8	3	10		
Natural Gas	2	8	1	8	3	10		

Ranking

Scenario		Criteria							Score
		Access to Agent	Knowledge/ Expertise	History of Threats (Building Functions/ Tenants)	Asset Visibility/ Symbolic	Asset Accessibility	Site Population/ Capacity	Level of Defense	
Chemical Agent									
Choking	Chlorine	5	7	3	8	3	10	5	40
	Phosgene	3	10	2	8	3	10	5	41
Blood	Hydrogen Cyanide	3	8	2	8	3	10	5	39
Blister	Lewisite	3	6	2	8	3	10	5	37
Nerve	Sarin	3	4	9	8	3	10	5	42

FEMA 452, Adaptation of Table 1-5: Nominal Example to Select Primary Threats for a Specific Urban Multi-story Building, p. 1-21

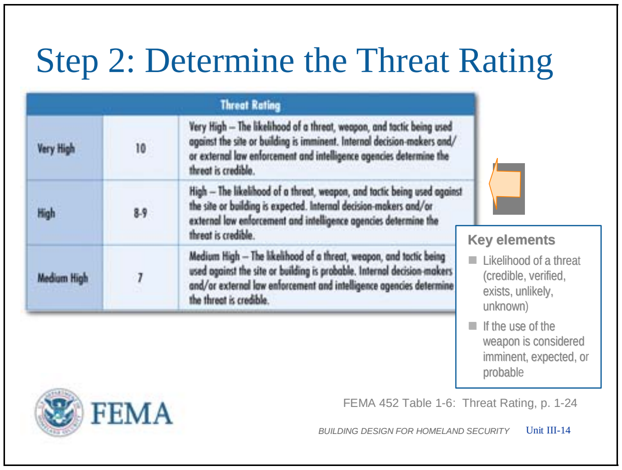
BUILDING DESIGN FOR HOMELAND SECURITY   Unit III-13

Selection of Primary Threats

This figure illustrates a nominal example of applying the threat scoring to blast and CBR. Note that the scores are first estimated for each criterion, and are then added on the far right column.

More sophisticated methods to score threats include Army-Air Force Technical Manual 5-853; State of Florida HLS-CAM (Homeland Security Comprehensive Assessment Model); and the DoD CARVER (criticality, accessibility, recuperability, vulnerability, effect, and recognizability) process. CARVER is a special operations forces acronym used throughout the targeting and mission planning cycle to assess mission validity and requirements. Essentially a military methodology that has similar parallels with a terrorist approach to targeting an asset.

VISUAL III-14



Step 2: Determine the Threat Rating

Threat Rating		
Very High	10	Very High – The likelihood of a threat, weapon, and tactic being used against the site or building is imminent. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is credible.
High	8-9	High – The likelihood of a threat, weapon, and tactic being used against the site or building is expected. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is credible.
Medium High	7	Medium High – The likelihood of a threat, weapon, and tactic being used against the site or building is probable. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is credible.

Key elements

- Likelihood of a threat (credible, verified, exists, unlikely, unknown)
- If the use of the weapon is considered imminent, expected, or probable

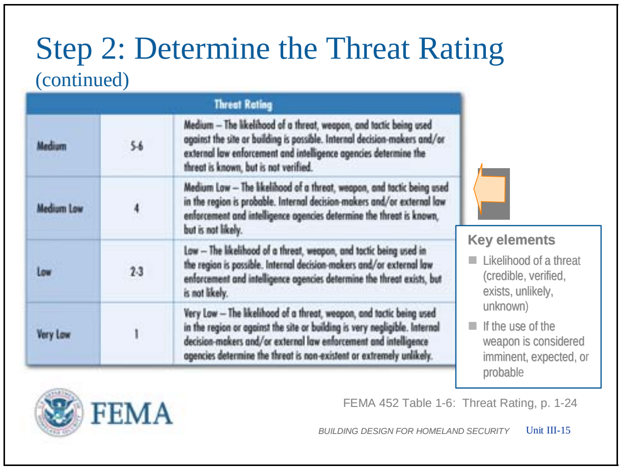
FEMA 452 Table 1-6: Threat Rating, p. 1-24

BUILDING DESIGN FOR HOMELAND SECURITY   Unit III-14

Step 2: Determine the Threat Rating
Having selected the primary threats for the building, the next step is to determine how the threat will affect the functions and critical infrastructure. The threat rating is an integral part of the risk assessment and is used to determine, characterize, and quantify a loss caused by an aggressor using a weapon or agent and tactic against the target (asset). The threat rating deals with the likelihood or probability of the threat occurring and the consequences of its occurrence.

This figure provides a scale for selecting your threat rating. Similar to the asset value scale (Unit II), the scale is a combination of a seven-level linguistic scale and a ten-point numerical scale. The key elements of this scale are likelihood / credibility of a threat, potential weapons to be used during a terrorist attack, and information available to decision-makers. This is a subjective analysis based on consensus opinion of the building stakeholders, threat specialists, and engineers. The primary objective is to look at the threat; the geographic distribution of functions and critical infrastructure; redundancy; and response and recovery to evaluate the impact on the organization should an attack occur.

VISUAL III-15



Step 2: Determine the Threat Rating
(continued)

Threat Rating		
Medium	5-6	Medium – The likelihood of a threat, weapon, and tactic being used against the site or building is possible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is known, but is not verified.
Medium Low	4	Medium Low – The likelihood of a threat, weapon, and tactic being used in the region is probable. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is known, but is not likely.
Low	2-3	Low – The likelihood of a threat, weapon, and tactic being used in the region is possible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat exists, but is not likely.
Very Low	1	Very Low – The likelihood of a threat, weapon, and tactic being used in the region or against the site or building is very negligible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is non-existent or extremely unlikely.

Key elements
- Likelihood of a threat (credible, verified, exists, unlikely, unknown)
- If the use of the weapon is considered imminent, expected, or probable

FEMA 452 Table 1-6: Threat Rating, p. 1-24

BUILDING DESIGN FOR HOMELAND SECURITY Unit III-15

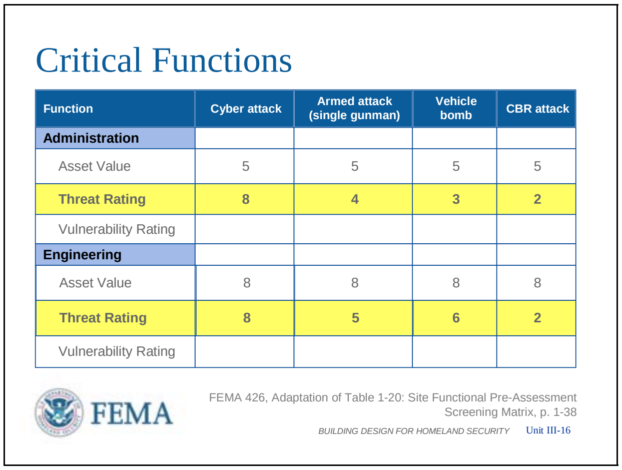
Step 2: Determine the Threat Rating (continued)

As explained on the previous slide, the threat rating includes the consequences of the threat occurrence.

- The consequences may be a feature attractive to the terrorist in their targeting philosophy.
- Conversely, threat and overall risk may be low, but if consequences are extremely high, then actions have been taken even against low threats and low risk because the organization did not want to contend with the consequences.

Thus, consequences may overtake perceived threat, especially if the threat is low. Think of the Murrah Federal Building threat rating before and after the McVeigh bombing and flying large aircraft into buildings before and after 9/11/2001.

VISUAL III-16



Critical Functions

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

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

BUILDING DESIGN FOR HOMELAND SECURITY Unit III-16

While the Asset Value of a Function or Infrastructure row is constant across all Threats / Hazards, the Threat / Hazard column may or may not be the same across all assets. The main reasons include whether or not the asset is being specifically targeted, the relative location

Critical Functions

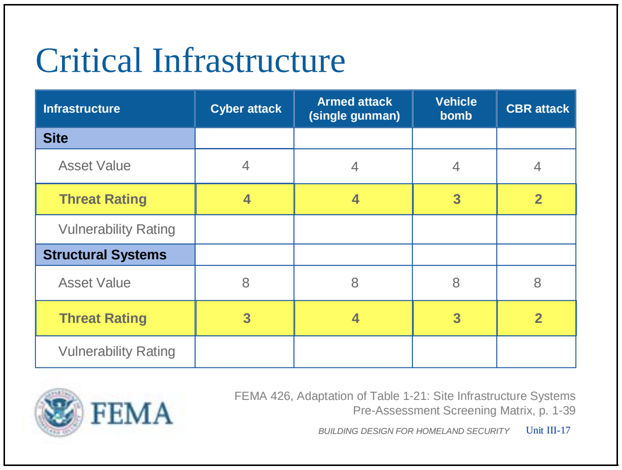
After each threat / hazard has been identified, the threat rating for each threat / hazard must be determined. The threat rating is a subjective judgment of a terrorist threat based on existence, capability, history, intentions, and targeting.

It is a snapshot in time, and can be influenced by many factors, but the given threat value will typically be the same for each function (going down the columns). Organizations that are dispersed in a campus environment may have variations.

On a scale of 1 to 10, 1 is a very low probability and 10 is a very high probability of a terrorist attack.

of the assets for that threat (vehicle bomb would have the same threat rating for all assets of a small footprint building, but not for a large footprint building) and the capability of use of the threat (Armed Attack, for example, would have a greater capability for assets on the exterior wall of a building or near an entrance vice assets in the core of a building behind multiple security/access control layers or non-observable layers. This is a fine line between threat and vulnerability – is a stand-off weapon armed attack a high threat because the terrorists have used this tactic or have the terrorists used the tactic because assets targeted were very susceptible to the attack method and thus were very vulnerable.

VISUAL III-17



Critical Infrastructure

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

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

BUILDING DESIGN FOR HOMELAND SECURITY Unit III-17

Following the same logic for determining threat ratings as explained on the previous slide, the threat rating to the site from Cyber Attack would be higher than structural systems because the access control or CCTV surveillance equipment across the site may be accessible from the internet. Structural systems are generally not connected to the internet or any electronic communication, except in the case of seismic dampers. The seismic dampers could be part of a “smart building” system where the responsive dampers are adjusted for the accelerations

Critical Infrastructure

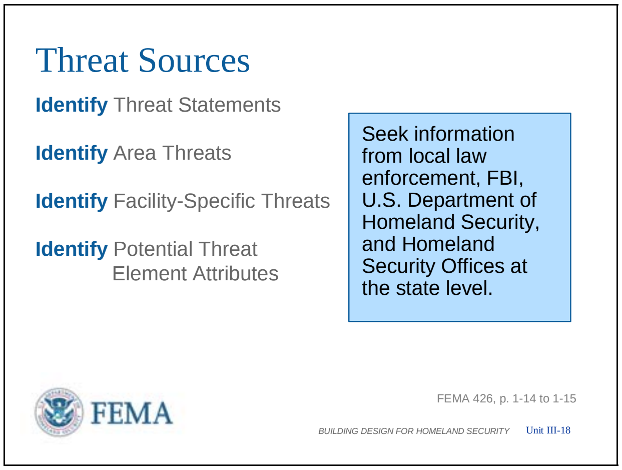
The Critical Infrastructure matrix has a similar threat rating approach as previously seen in the Critical Function matrix.

Note that the threat ratings for the Site and Structural Systems are almost identical, only varying for Cyber Attack as explained in the left-hand column.

The other threat ratings for Site and Structural Systems are on the low side of the scale because the targeting value to the terrorist and the consequences of using that attack mode on that asset are relatively low.

imposed upon the structure, especially high-rises.

VISUAL III-18



Threat Sources

Identify Threat Statements

Identify Area Threats

Identify Facility-Specific Threats

Identify Potential Threat Element Attributes

Seek information from local law enforcement, FBI, U.S. Department of Homeland Security, and Homeland Security Offices at the state level.

FEMA 426, p. 1-14 to 1-15

BUILDING DESIGN FOR HOMELAND SECURITY Unit III-18

Exam Questions #A3 and B4

Note: For technological hazards, it is also important to gather information from the local fire department and hazardous materials (HazMat) unit, Local Emergency Planning Committee (LEPC), and State Emergency Response Commission (SERC). LEPC and SERC are local and state organizations established under a U.S. Environmental Protection Agency (EPA) program. They identify critical facilities in vulnerable zones and generate emergency management plans. Additionally, most fire departments understand which industries in the local area handle the most combustible materials and the HazMat unit understands who handles materials that could have a negative impact upon people and the environment. In many jurisdictions, the HazMat unit is part of the fire department.

Threat Sources

A manmade threat / hazard analysis requires coordination with security and intelligence organizations that understand the locality, the region, and the Nation. These organizations include the police department (whose jurisdiction includes the building or site), the local state police office, and the local office of the FBI. In many areas of the country, there are threat-coordinating committees, including FBI Joint Terrorism Task Forces, which facilitate the sharing of information. Computer systems are also in place to disseminate intelligence information down to the lowest levels and up to the highest levels.

Other sources of potential threat information are available on the internet, such as the Southern Poverty Law Center, which tracks hate groups in the United States, at their web site: www.splcenter.org.

VISUAL III-19

Design Basis Threat

The threat against which assets within a building must be protected and upon which the security engineering design of the building is based.

BUILDING DESIGN FOR HOMELAND SECURITY Unit III-19

Note: Facility designers need to have the size and type of bomb, vehicle, gun, CBR, or other threat tactic, weapon, or tool identified in order to provide an appropriate level of protection.

There are several methodologies and assessment techniques that can be used. Historically, the U.S. military methodology (with a focus on explosive effects, CBR, and personnel protection) has been used extensively for military installations and other national infrastructure assets.

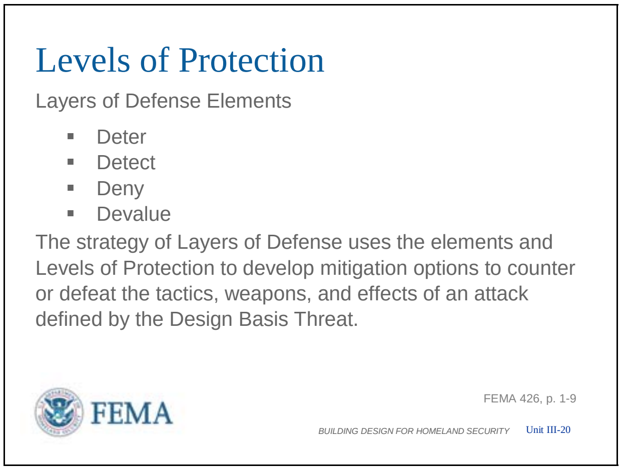
- The Department of State (DOS) adopted or co-developed many of the same blast and CBR design criteria as DoD and GSA.
- The GSA further developed criteria for Federal buildings as a result of the attack on the Murrah Federal Building.
- The Department of Commerce (DOC) Critical Infrastructure Assurance Office (CIAO) established an assessment framework, which focused on information technology infrastructure.

Design Basis Threat

We first applied a systems engineering evaluation process to determine a building's critical functions and critical infrastructure. Then we achieve an understanding of the aggressors' likely weapons and attack delivery mode. The next step in the process of quantifying a building's risk assessment is determining the "Design Basis Threat" – the minimum threat tactic that the designers and engineers use in designing a new structure or renovation. The final step in this threat process is the senior management selection of the "Level of Protection" which is also required by the designers and engineers as part of the building design or renovation.

After review of the preliminary information about the building functions, infrastructure, and threats, senior management should establish the "Design Basis Threat" and select the desired "Level of Protection."

VISUAL III-20



Levels of Protection

Layers of Defense Elements

- Deter
- Detect
- Deny
- Devalue

The strategy of Layers of Defense uses the elements and Levels of Protection to develop mitigation options to counter or defeat the tactics, weapons, and effects of an attack defined by the Design Basis Threat.

FEMA 426, p. 1-9

BUILDING DESIGN FOR HOMELAND SECURITY Unit III-20

Levels of Protection (1/3)

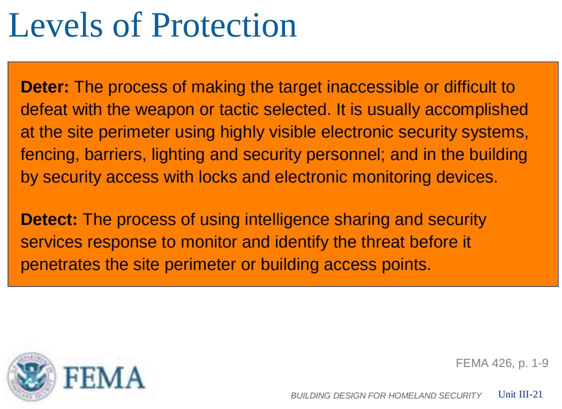
Layers of Defense elements, that along with Levels of Protection, provide the strategy for developing mitigation options.

- Deter
- Detect
- Deny
- Devalue

Let’s look at these in more detail on the next slides.

Exam Questions #A18 and B17

VISUAL III-21



Levels of Protection

Deter: The process of making the target inaccessible or difficult to defeat with the weapon or tactic selected. It is usually accomplished at the site perimeter using highly visible electronic security systems, fencing, barriers, lighting and security personnel; and in the building by security access with locks and electronic monitoring devices.

Detect: The process of using intelligence sharing and security services response to monitor and identify the threat before it penetrates the site perimeter or building access points.

FEMA 426, p. 1-9

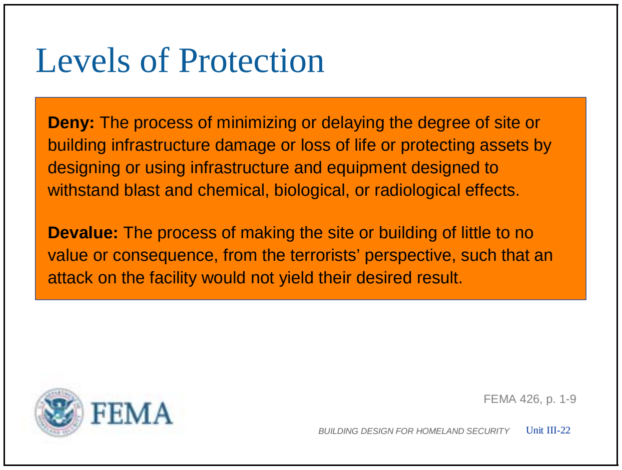
BUILDING DESIGN FOR HOMELAND SECURITY Unit III-21

Levels of Protection (2/3)

Layers of Defense elements

- Deter
  - Harden the perimeter or building in a fashion that the terrorist will not think the available tactics will work against the asset
  - This can be perceived hardening by the terrorist doing target planning vice actual hardening, such as a dog at an access control point
  - Preferably done at a significant distance from the asset
- Detect
  - Identify the attempted access or preparation of a tactic prior to reaching the asset or where the tactic can be employed
  - Usually done in conjunction with Deny as explained on the next slide

VISUAL III-22



Levels of Protection

Deny: The process of minimizing or delaying the degree of site or building infrastructure damage or loss of life or protecting assets by designing or using infrastructure and equipment designed to withstand blast and chemical, biological, or radiological effects.

Devalue: The process of making the site or building of little to no value or consequence, from the terrorists' perspective, such that an attack on the facility would not yield their desired result.

FEMA 426, p. 1-9

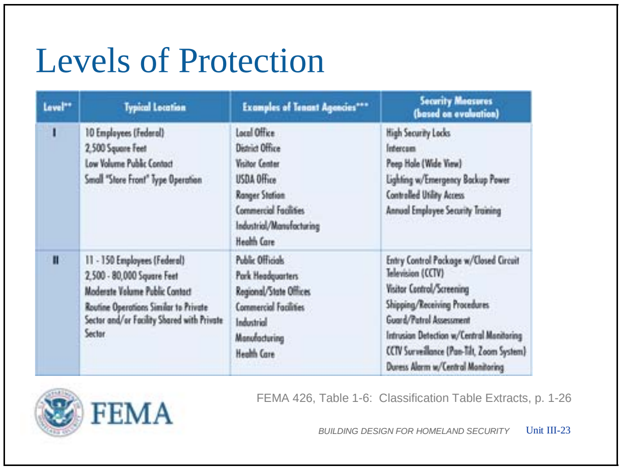
BUILDING DESIGN FOR HOMELAND SECURITY Unit III-22

Levels of Protection (3/3)

Layers of Defense elements

- Deny
  - In conjunction with Detect, a security evaluation is made and a response is initiated to delay or capture aggressors or deny their access to their target.
  - Hardening the asset so as to withstand the employment of the tactic without detriment to people, critical functions, or critical infrastructure
- Devalue
  - Make the asset a less desirable actual or perceived target by dispersing, camouflage, concealment, or deception

VISUAL III-23



Levels of Protection

Level**	Typical Location	Examples of Tenant Agencies***	Security Measures (based on evaluation)
I	10 Employees (Federal) 2,500 Square Feet Low Volume Public Contact Small "Store Front" Type Operation	Local Office District Office Visitor Center USDA Office Ranger Station Commercial Facilities Industrial/Manufacturing Health Care	High Security Locks Intercom Peep Hole (Wide View) Lighting w/Emergency Backup Power Controlled Utility Access Annual Employee Security Training
II	11 - 150 Employees (Federal) 2,500 - 80,000 Square Feet Moderate Volume Public Contact Routine Operations Similar to Private Sector and/or Facility Shared with Private Sector	Public Officials Park Headquarters Regional/State Offices Commercial Facilities Industrial Manufacturing Health Care	Entry Control Package w/Closed Circuit Television (CCTV) Visitor Control/Screening Shipping/Receiving Procedures Guard/Patrol Assessment Intrusion Detection w/Central Monitoring CCTV Surveillance (Pan-Tilt, Zoom System) Duress Alarm w/Central Monitoring

FEMA 426, Table 1-6: Classification Table Extracts, p. 1-26

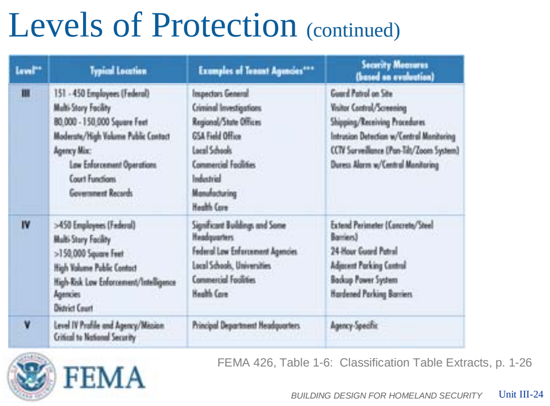
BUILDING DESIGN FOR HOMELAND SECURITY Unit III-23

Levels of Protection (1/2)

This table – extracted from the U.S. Department of Justice's *Vulnerability Assessment of Federal Facilities* (1995) – presents a series of security measures for typical sizes and types of sites, in addition to a transferable example of appropriate security measures for typical locations and occupancies.

Here is the lower end of the Levels of Protection which is a quick assessment of asset value, critical functions and critical infrastructure and the physical security measures that a security professional would select from to apply.

VISUAL III-24



Levels of Protection (continued)

Level**	Typical Location	Examples of Tenant Agencies***	Security Measures (based on evaluation)
III	151 - 450 Employees (Federal) Multi-Story Facility 80,000 - 150,000 Square Feet Moderate/High Volume Public Contact Agency Mix: Law Enforcement Operations Court Functions Government Records	Inspectors General Criminal Investigations Regional/State Offices GSA Field Office Local Schools Commercial Facilities Industrial Manufacturing Health Care	Guard Patrol on Site Visitor Control/Screening Shipping/Receiving Procedures Intrusion Detection w/Central Monitoring CCTV Surveillance (Pan-Tilt/Zoom System) Duress Alarm w/Central Monitoring
IV	>450 Employees (Federal) Multi-Story Facility >150,000 Square Feet High Volume Public Contact High-Risk Law Enforcement/Intelligence Agencies District Court	Significant Buildings and Some Headquarters Federal Law Enforcement Agencies Local Schools, Universities Commercial Facilities Health Care	Extend Perimeter (Concrete/Steel Barriers) 24-Hour Guard Patrol Adjacent Parking Control Backup Power System Hardened Parking Barriers
V	Level IV Profile and Agency/Mission Critical to National Security	Principal Department Headquarters	Agency-Specific

FEMA 426, Table 1-6: Classification Table Extracts, p. 1-26

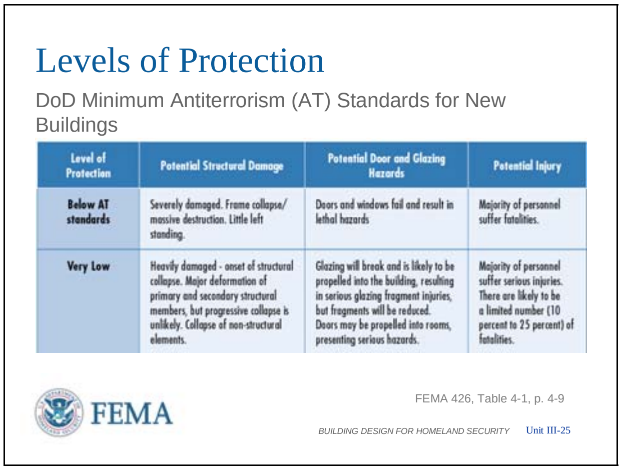
FEMA

BUILDING DESIGN FOR HOMELAND SECURITY Unit III-24

Levels of Protection (1/2)

This is the upper end of the table, with associated higher asset value, greater targeting potential, greater consequences, and significantly greater physical security measures.

VISUAL III-25



Levels of Protection

DoD Minimum Antiterrorism (AT) Standards for New Buildings

Level of Protection	Potential Structural Damage	Potential Door and Glazing Hazards	Potential Injury
Below AT standards	Severely damaged. Frame collapse/ massive destruction. Little left standing.	Doors and windows fail and result in lethal hazards	Majority of personnel suffer fatalities.
Very Low	Heavily damaged - 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.

FEMA 426, Table 4-1, p. 4-9

FEMA

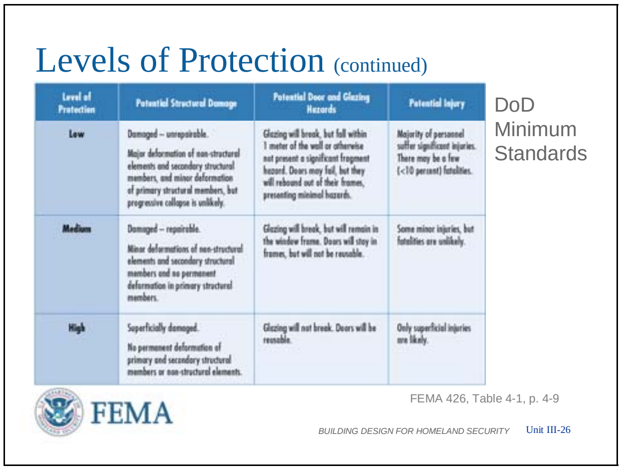
BUILDING DESIGN FOR HOMELAND SECURITY Unit III-25

Levels of Protection
DoD Minimum Antiterrorism (AT) Standards for New Buildings (1/2)

In contrast to the GSA security levels and criteria, the DoD correlates levels of protection with potential damage and expected injuries.

At the levels shown here, there is significant damage, injury, and an estimated number of dead.

VISUAL III-26



Levels of Protection (continued)

Level of Protection	Potential Structural Damage	Potential Door and Glazing Hazards	Potential Injury
Low	Damaged – 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 (<10 percent) fatalities.
Medium	Damaged – 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 injuries, but fatalities are unlikely.
High	Superficially damaged. 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.

DoD Minimum Standards

FEMA 426, Table 4-1, p. 4-9

FEMA

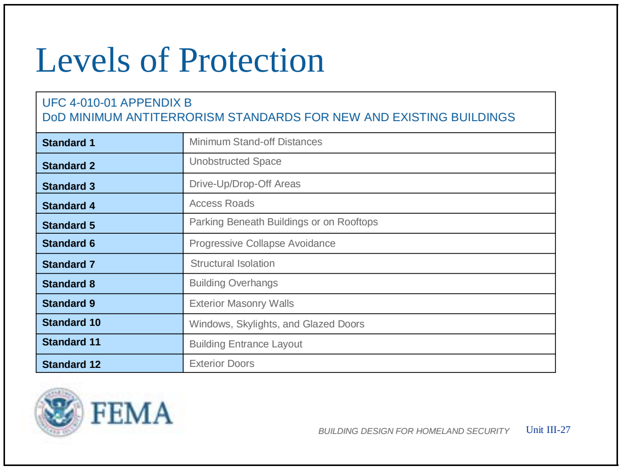
BUILDING DESIGN FOR HOMELAND SECURITY Unit III-26

Levels of Protection
DoD Minimum Antiterrorism (AT) Standards for New Buildings (2/2)

A low level of protection should be the minimum sought in a design using the "Design Basis Threat" for hardening. Few fatalities are expected.

Medium and high levels of protection will cost more to achieve.

VISUAL III-27



Levels of Protection

UFC 4-010-01 APPENDIX B DoD MINIMUM ANTITERRORISM STANDARDS FOR NEW AND EXISTING BUILDINGS	
Standard 1	Minimum Stand-off 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, Skylights, and Glazed Doors
Standard 11	Building Entrance Layout
Standard 12	Exterior Doors

BUILDING DESIGN FOR HOMELAND SECURITY Unit III-27

Levels of Protection

DoD Antiterrorism Standards 1 to 12.

Highlight Standards 1, 2, and 4, and refer to **the Building Vulnerability Assessment Checklist** questions for blast evaluation.

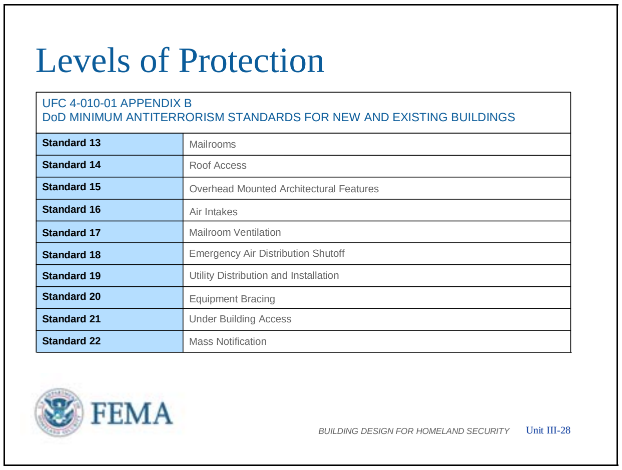
- DOD Std 1 – Minimum Stand-off Distance
  - Separation distance – vehicle bomb to building
  - Analysis to show level of protection achieved if minimum stand-off cannot be met

- DoD Std 2 – Unobstructed Space
  - Clear Zone around building preventing a package bomb from being hidden
  - No equipment or enclosures within unobstructed space

- DoD Std 4 – Access Roads
  - Access control measures that ensure unauthorized vehicles do not get inside the minimum stand-off distance

Each standard correlates to a Level of Protection and Design Basis Threat.

VISUAL III-28



Levels of Protection

UFC 4-010-01 APPENDIX B DoD MINIMUM ANTITERRORISM STANDARDS FOR NEW AND EXISTING BUILDINGS	
Standard 13	Mailrooms
Standard 14	Roof Access
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

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY Unit III-28

Levels of Protection

DoD Antiterrorism Standards 13 to 22.

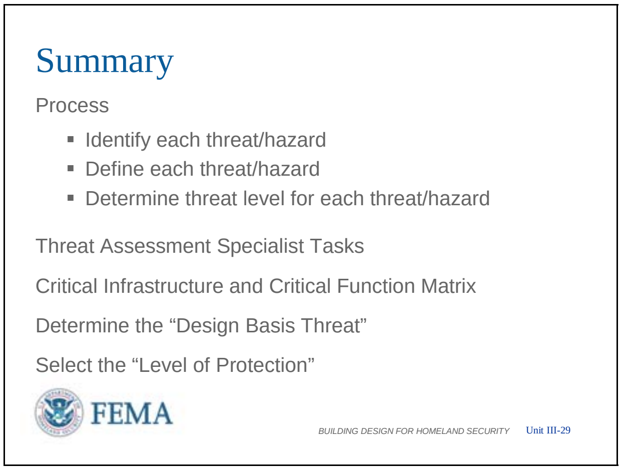
Highlight Standards 16, 17, and 18, and the impacts on HVAC.

- DOD Std 16 – Air Intakes
  - Prevent easy introduction of CBR agents into the HVAC system

- DoD Std 17 – Mailroom Ventilation
  - Separate HVAC system serving only the mailroom
  - Configure room pressures so that mailroom is at a lower pressure than other adjacent parts of building and air leakage only comes <u>into</u> the mailroom, preventing spread of contaminants until HVAC system is shut down

- DoD Std 18 – Emergency Air Distribution Shutdown
  - Immediately shut down air distribution throughout building except where interior pressure and airflow control would more efficiently prevent spread of airborne contaminants and/or ensure the safety of egress pathways.

VISUAL III-29



Summary

Process

- Identify each threat/hazard
- Define each threat/hazard
- Determine threat level for each threat/hazard

Threat Assessment Specialist Tasks

Critical Infrastructure and Critical Function Matrix

Determine the "Design Basis Threat"

Select the "Level of Protection"

FEMA
BUILDING DESIGN FOR HOMELAND SECURITY
Unit III-29

Summary

The process for developing threat assessments:

- Identify each threat / hazard
- Define each threat / hazard
- Determine threat level for each threat / hazard

Use Federal, state, or local law enforcement to help determine threat ratings.

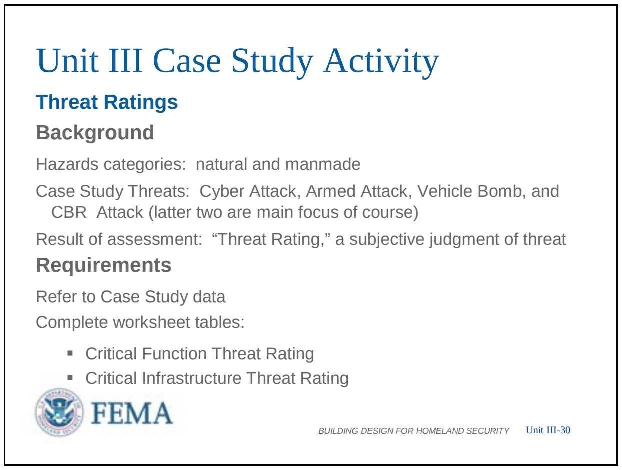
Complete the Critical Functions and Critical Infrastructure Matrices.

Establish the Design Basis Threat.

Select the Level of Protection.

Use Layers of Defense strategy to mitigate attack and develop mitigation options.

VISUAL III-30



Unit III Case Study Activity

Threat Ratings

Background

Hazards categories: natural and manmade

Case Study Threats: Cyber Attack, Armed Attack, Vehicle Bomb, and CBR Attack (latter two are main focus of course)

Result of assessment: "Threat Rating," a subjective judgment of threat

Requirements

Refer to Case Study data

Complete worksheet tables:

- Critical Function Threat Rating
- Critical Infrastructure Threat Rating

Refer participants to **FEMA 426** and the Unit III Case Study activity in the Student Manual.

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

Student Activity

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
- Manmade

To focus the class and improve the learning experience by eliminating excessive variation among threats, the Case Study is limited to four threats as shown on the Risk Matrix:

- Cyber attack
- Armed attack
- Explosive blast
- Chemical, biological, and/or radiological "agents"

At the end of 30 minutes, reconvene the class.

The plenary session to facilitate group reporting has 15 minutes to go through and discuss the answers.

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
- Targeting

The rating scale is a scale of 1 to 10:

- 1 is a very low probability of a terrorist attack
- 10 is a very high probability.

Activity Requirements

Working in small groups, refer to the Case Study and complete the worksheet tables for:

- Critical Functions
- Critical Infrastructure

Take 30 minutes to complete this activity. Solutions will be reviewed in plenary group.

Transition

Unit IV will cover Vulnerability Assessment and Unit V will cover Risk Assessment / Risk Management.

This page intentionally left blank.

UNIT III-A CASE STUDY ACTIVITY: THREAT/HAZARD RATING (Suburban Version)

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. Although 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."

To complete the threat assessment, the two-step process has been selected. Step 1 is to identify the primary threats according to criteria shown on the following page.

For the sake of this course, the four primary threats have been determined to be Cyber Attack, Armed Attack, Vehicle Bomb, and CBR Attack. However, to familiarize yourself with the process of determining the primary threats, determine the threat score for a 500-lb. vehicle bomb.

The second step of the threat assessment process is the determination of the "Threat Rating." 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 would impact the entire facility.

Step 1: Determine the score for a 500-lb. vehicle bomb

Criteria
Improvised Explosive Device (Bomb)

- Level of Defense – Little or no defense against threats. No specific security design taken into consideration or adopted for this threat.

FEMA 452 Criteria

Step 2: Determine the threat rating for HIC

HIC Critical Functions Threat Rating

1. Administration	8	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	8	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
3. Loading Dock / Warehousing	8	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
4. Data Center	8	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
5. Communications	8	3	6	4	Digital communications tend to have a higher threat rating than analog communication

					systems because analog communications are generally hardwired and not connected to internet. Access by wireless or telephone call up would increase the threat rating by increasing accessibility with wireless having a higher threat rating than telephone call up.
6. Security	8	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
7. Housekeeping	8	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.

HIC Infrastructure Threat Rating

1. Site	1	3	6	4	Local and international groups with the capability, intentions,

					and targeting expertise are known to be in the area.
2. Architectural	1	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
3. Structural	1	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
4. Envelope Systems	1	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
5. Utility Systems	5	5	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
6. Mechanical Systems	5	5	6	4	Local and international

					groups with the capability, intentions, and targeting expertise are known to be in the area.
7. Plumbing and Gas Systems	1	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
8. Electrical Systems	5	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
9. Fire Alarm Systems	2	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
10. IT / Communications Systems	10	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are

					known to be in the area.

UNIT III-B CASE STUDY ACTIVITY:
THREAT / HAZARD RATING
(Urban Version)

After assets that need to be protected are determined, the next step is to identify the threats and hazards that could harm the building and its inhabitants. Hazards are categorized into two groups: natural and manmade. For the sake of this course, the four primary threats selected are Cyber Attack, Armed Attack, Vehicle Bomb, and CBR Attack.

Requirements

Refer to the Appendix B Case Study data and complete the following worksheets. Each student as part of their assessment team will interpret the HZC threat information and should select and justify a threat/hazard rating number with rationale.

- Any function with key IT systems connected to the Internet should get high cyber threat values.
- The threat of explosive blast should be looked upon as either as directly targeted or as collateral damage. Before giving a consistently low rating, consider your answer to Step 1 below as it would have been applied to the Murrah Building in Oklahoma City in 1995.
- A CBR attack or nearby HazMat spill could impact the entire facility, but to varying degrees by floors in a 50-story building if the agent is heavier or lighter than air.

Thus, to illustrate threat assessment, two separate steps were selected for their different methodology.

- Step 1 uses the FEMA 452 Criteria that has its basis in the rating process developed by the US Marshals Service after the Murrah Building bombing in Oklahoma City. The US Marshals Service process was then used by GSA to begin assessing Federal buildings. This method tends to look at the building as a whole.

- Step 2 uses the FEMA 426 methodology of applying a threat rating using specific or generic tactics in a given threat scenario against a specific asset, such as critical functions or critical infrastructure. Thus, this method tends to look at the various components of the building so as to focus limited resources to achieve maximum risk reduction by taking care of the most critical assets.

Final Action: Transfer answers from the Threat Rating tables below to the Risk Matrix poster after team agreement on team answer.

Step 1: Determine the threat score for a 500-lb. vehicle bomb as applied to HZC

Familiarize yourself with the process of determining the primary threats according to the FEMA 452 criteria (**Table 1-4, page 1-21, FEMA 452**) by determining the threat score for a 500-lb. (TNT equivalent) vehicle bomb using the information on the next page and in the Appendix B Case Study.

As shown in Table 1-5, page 1-22, FEMA 453, you can use this scoring methodology to determine your primary threats based upon the threats that achieve the highest scores. However note that the criteria actually intersperses Asset Value Rating, Threat Rating, and Vulnerability Rating as indicated below:

- Access to Agent (Threat – capability of potential threat elements)
- Knowledge/Expertise (Threat – capability of potential threat elements)
- History of Threats/Actual Usage (Threat – rhetoric and actual use by potential threat elements)
- Asset Visibility / Symbolic (Asset Value – but in eyes of potential threat elements as target)
- Asset Accessibility (Vulnerability)
- Site Population / Capacity (Asset Value or Threat (Targeting))
- Level of Defense (Vulnerability)

FEMA 452 Table 1-4 Criteria
Improvised Explosive Device (Bomb)

Rationale for Above Numbers using FEMA 452 Criteria on next page

“Farm” explosives

- Access to Agent -- Readily available
- Knowledge/Expertise --Instructions on internet
- History gets a higher rating closer to home -- Regional/State good choice for urban environment
- Asset Visibility / Symbolic– well known, but not a landmark
- Asset Accessibility – currently open access, unrestricted underground parking
- Site Population – 9,000 average
- Level of Defense – Little or no defense against threats. No specific security design taken into consideration or adopted for this threat.

FEMA 452 Criteria

K

Step 2: Determine Threat Ratings for HazardCorp Building

The second step is the FEMA 426 method for determining the "Threat Rating." The rating scale is a scale of 1 to 10, with 1 being a very low probability of a terrorist attack and 10 a very high probability.

NOTE 1: In the previous student activity to determine Asset Value Rating, there was only one value of an asset – it did not change based upon threat or situation. The impact if the asset was damaged or lost is a view of its value.

NOTE 2: In like manner, the Threat Rating will tend to be the same across all assets. Variances can occur across large buildings where all functions may not exist in all portions of the building or the targeting of the asset may be negligible – no history, no capability – such as Cyber Attack against an asset that has no computer and no connection to the internet. This can be called a very low threat, but it also indicates that since cyber attack cannot occur, the asset has no vulnerabilities to that threat.

HZC Critical Functions Threat Rating

1. Administration	6	6	9	6	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
2. Engineering / IT Technicians	6	4	9	6	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
3. Loading Dock / Warehousing	6	7	9	6	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.

4. Data Center	6	3	9	6	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
5. Communications	6	4	9	6	Digital communications tend to have a higher threat rating than analog communication systems because analog communications are generally hardwired and not connected to internet. Access by wireless or telephone call up would increase the threat rating by increasing accessibility with wireless having a higher threat rating than telephone call up.
6. Security	6	7	9	6	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
7. Housekeeping	2	2	9	6	Local and international

					groups with the capability, intentions, and targeting expertise are known to be in the area.

HZC Infrastructure Threat Rating

1. Site	1	3	9	6	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
2. Architectural	1	3	9	6	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
3. Structural	1	3	9	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
4. Envelope Systems	1	3	9	6	Local and international groups with the capability, intentions,

					and targeting expertise are known to be in the area.
5. Utility Systems	1	3	9	6	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
6. Mechanical Systems	5	3	9	6	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
7. Plumbing and Gas Systems	1	3	9	6	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
8. Electrical Systems	5	5	9	6	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
9. Fire Alarm Systems	2	2	9	6	Local and international

					groups with the capability, intentions, and targeting expertise are known to be in the area.
10. IT / Communications Systems	8	4	9	6	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.

This page intentionally left blank